Universidade Federal de Pernambuco
Centro de Tecnologia e Geociências
Curso de Especialização em Engenharia de Instrumentação

Avaliação da utilização de tecnologia de comunicação sem fio em redes PROFIBUS e FOUNDATION Fieldbus™

Leonardo Tavares do Nascimento

Orientador: Prof. José Sérgio da Rocha Neto D. Sc.

Monografia apresentada ao Centro de Tecnologia e Geociências da Universidade Federal de Pernambuco como parte dos requisitos para obtenção do Certificado de Especialista em Engenharia de Instrumentação

Recife, 2008

Resumo

Avaliação da utilização de tecnologia de comunicação sem fio em redes PROFIBUS e FOUNDATION Fieldbus™

Leonardo Tavares do Nascimento

Março/2008

Orientador: Prof. José Sérgio da Rocha Neto D. Sc.
Área de concentração: Eletrônica
Palavras-chaves: automação, redes industriais, comunicação sem fio

Na automação industrial, o uso de redes de comunicação tem sido importante para as melhorias das ações de controle e de monitoramento. Objetiva-se com as redes de campo permitir uma maior integração entre o nível de gerenciamento e o nível de supervisão da planta industrial com os controladores e instrumentos de campo. Dentre as principais redes industriais em uso, a PROFIBUS e a FOUNDATION Fieldbus se destacam pelo crescimento no número de instalações, especialmente na área de controle de processos (indústrias químicas e petroquímicas).

A tecnologia de transmissão, utilizando-se redes de comunicação sem fio vem conquistando espaço, devido às vantagens associadas como redução de cabos e mobilidade. Nas aplicações industriais, o padrão ZigBee possui características que o tornam atrativo.

A utilização de redes de comunicação sem fio na automação industrial esbarra nas limitações dessas tecnologias e na necessidade de modificar as infra-estruturas operantes. Devido às propriedades especiais da transmissão sem fio, não é desejável que todos os nós de uma rede industrial *fieldbus* sejam sem fio. Também ainda não é recomendável utilizar esta tecnologia de comunicação em aplicações de controle críticas, remanescendo a monitoração como principal área de atuação dos sistemas sem fio. Desta forma, uma solução híbrida abrangendo a coexistência de transmissão por cabos e transmissão sem fio se torna mais atraente. Neste caso, os dispositivos cabeados precisam se comunicar com os nós sem fio, trazendo a necessidade de formas de interconexão.

O objetivo deste trabalho é investigar as formas de interconexão entre redes industriais *fieldbus* e redes de sensores sem fio, mais especificamente a integração de redes PROFIBUS e FOUNDATION Fieldbus com redes sem fio no padrão ZigBee, analisando características, propriedades e restrições existentes.

Conteúdo

1. Introdução

No mercado atual globalizado, em que há uma busca por vantagens tecnológicas que permitam ao seu usuário competir de maneira eficaz, a automação industrial passou a ser um requisito. No ramo da indústria do petróleo, especialmente no segmento do refino, a otimização de recursos e redução de custos faz-se imprescindível. As inovações na área de processo em si são poucas, ficando para as áreas de controle e instrumentação a responsabilidade por alcançar tais objetivos.

A necessidade de a informação poder ser disponibilizada em vários locais simultaneamente, mostrando resultados em tempo real da cadeia de produção, faz com que as redes de comunicação de dados estejam cada vez mais presentes no cotidiano industrial, ocasionando uma constante busca por novas técnicas e meios de estabelecer essa comunicação.

A instrumentação em rede constitui um conceito interessante no domínio industrial, na medida em que permite a distribuição do processamento e controle pelos diversos instrumentos que estão ligados à rede. Dá-se o nome de redes industriais *fieldbus* aos sistemas de controle industrial com este tipo de arquitetura. Uma característica muito importante em muitas destas redes é a sua interoperabilidade, ou seja, a possibilidade do instrumento de um fabricante poder ser substituído por outro de qualquer fabricante, com a conservação de todas as características funcionais.

À medida que os benefícios das redes industriais *fieldbus* se tornam mais aparentes, cresce o número de usuários adeptos desta tecnologia. Espera-se que o mercado mundial de soluções *fieldbus* na indústria de processos cresça a taxas anuais de 22,3% nos próximos cinco anos. A movimentação financeira neste mercado foi maior que US$ 831 milhões em 2006 e há previsões que possa ultrapassar os US$ 2,279 bilhões em 2011, de acordo com um estudo realizado pela ARC Advisory Group [39].

Atualmente o número de nós (estações, dispositivos) por instalação está crescendo drasticamente. Essa evolução acontece em conjunto com os avanços das redes de sensores. Os progressos tecnológicos dos sistemas micro-eletromecânicos (MEMS – *micro-electromechanical systems*) têm provocado mudanças em ambientes industriais de forma intensa. A cada dia, novos dispositivos de tamanhos reduzidos e com elevada capacidade de atuação estão sendo encontrados no mercado. Novos protocolos de comunicação também têm trazido vários benefícios para as indústrias em geral [29]. Se extrapolarmos a experiência de outros campos da tecnologia, podemos tentar desenhar a próxima evolução: os preços dos dispositivos irão cair, e ao mesmo tempo a performance irá crescer, permitindo a integração de cada vez mais inteligência aos instrumentos. Assim, poderemos ter redes complexas com cerca de um milhão de nós trabalhando juntos [6]. Tais

sistemas serão os desafios nas próximas décadas.

A mais promissora área de investigação para a evolução tecnológica é o domínio sem fio [6]. Pesquisa realizada no ano de 2005 pela ON World Inc. [26], com grande parte das maiores companhias de petróleo e gás natural do mundo, revelou que todas as empresas pesquisadas adotam tecnologia sem fio acoplada em seus sistemas supervisórios e planejavam, em curto prazo, investimento em tecnologia de monitoramento remoto para suas plantas industriais. Os benefícios no uso de tal tecnologia são: ausência de cabeamento propenso a falhas, alta flexibilidade, e até mesmo mobilidade. Os problemas também existem: atenuação, desvanecimento, multipercurso, estações temporariamente ocultas, e o simples acesso de intrusos. Até agora, as opções de comunicação sem fio têm sido usadas apenas para substituir o cabeamento de dados convencional [6]. Um uso eficiente da comunicação sem fio necessitaria de uma redefinição de pelo menos a camada inferior das redes industriais *fieldbus*. A avaliação das tecnologias sem fio disponíveis com relação à sua aplicabilidade em automação é o primeiro passo nessa direção.

Neste capítulo é apresentado o conceito de automação industrial e sua evolução histórica, tratando sobre redes industriais e tecnologia de transmissão sem fio. Uma definição mais detalhada sobre redes industriais *fieldbus* é realizada no Capítulo 2, que também esclarece o motivo da escolha das redes PROFIBUS e FOUNDATION Fieldbus, descrevendo as características de ambas. O Capítulo 3 aborda a utilização de tecnologias de transmissão sem fio em ambientes industriais, citando os padrões existentes, expondo o porquê da escolha do ZigBee, e detalhando as propriedades deste padrão. As minúcias da interconexão entre as redes industriais *fieldbus* escolhidas e redes sem fio que adotem o padrão ZigBee, relatando as possíveis formas de realização, os requisitos e as limitações, são encontradas no Capítulo 4. Por fim, é feita uma avaliação geral do estudo realizado, apontando os aspectos relevantes observados.

1.1. Automação industrial

Automação é o uso de qualquer dispositivo mecânico ou eletro-eletrônico para controlar máquinas e processos, podendo ser realizado por um computador, que substitua o trabalho humano em favor da qualidade dos produtos, da redução dos custos, da rapidez da produção ou da segurança das pessoas, assim aperfeiçoando os complexos objetivos das indústrias e serviços.

Atualmente, envolve a implantação de sistemas interligados e assistidos por redes de comunicação, compreendendo sistemas supervisórios e interfaces humano-máquina que possam auxiliar os operadores na supervisão e análise dos problemas.

Na Figura 1 representa-se a chamada pirâmide de automação, com os diferentes níveis de automação encontrados em uma planta industrial. A pirâmide pode ser descrita em cinco níveis [1]:

- **Nível 1**: dispositivos de campo, como sensores e atuadores;

- **Nível 2**: nível dos controladores (CLPs) e de algum tipo de supervisão associada ao processo;
- **Nível 3**: permite o controle do processo produtivo da planta, normalmente constituído por banco de dados;
- **Nível 4**: responsável pela programação e pelo planejamento da produção;
- **Nível 5**: administração dos recursos da empresa, em que se encontra a gestão de todo o sistema.

As redes de campo ocupam os dois níveis inferiores da pirâmide de automação.
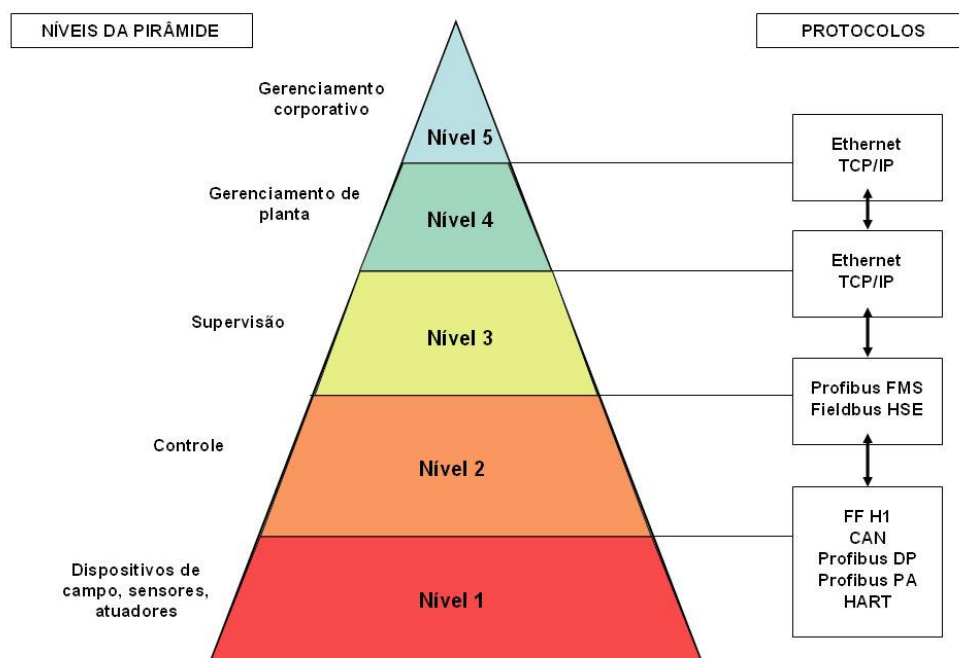
Figura 1 - A pirâmide de automação

Para grandes aplicações existe a necessidade de se estabelecer um critério de como será feita a aquisição de dados utilizando-se de CLPs, de estações remotas e demais equipamentos inteligentes do chão de fábrica. Uma maneira simples de fazer isso é colocar todas as *interfaces* para se comunicar com os equipamentos. Isso gera baixo desempenho de comunicação, uma vez que todos os computadores precisam acessar os dados ao mesmo tempo. Outra forma é um sistema acessando os dados dos CLPs e disponibilizando-os para outros sistemas através de uma rede de computadores, totalmente independente da rede de CLPs, utilizando-se por exemplo, sistemas configuráveis SCADA (*Supervisory Control and Data Acquisition*) que são destinados à supervisão, ao controle e à aquisição de dados em plantas industriais, sendo muito populares [1].

A utilização dos microprocessadores na indústria possibilitou a realização do controle digital centralizado, que possui as seguintes características: cabeamento paralelo utilizando fios em

par trançado e topologia estrela; transmissão de dados entre os dispositivos (sensores e atuadores) e a unidade de controle, na forma de sinais analógicos e digitais. A grande quantidade de dispositivos e as longas distâncias causam altos custos de instalação e manutenção. Outra limitação é a falta de flexibilidade para extensões ou modificações. Para superar essas dificuldades, foram desenvolvidos sistemas de automação de controle centralizado e barramento. Nesse sistema a estação de controle comunica-se com os dispositivos através de um barramento. Suas características são: controle centralizado e transmissão digital em topologia de barramento. O avanço na tecnologia e a demanda do mercado levaram ao desenvolvimento de sistemas de controle conhecidos como barramento de campo distribuído. As características desses sistemas são: inteligência distribuída, usando microcontroladores ao longo do barramento; redução de cabeamento; unidades de conexão (*gateways*, pontes, repetidores, etc.). Atualmente, implementando melhorias em relação a esses sistemas, foram desenvolvidos os chamados sistemas de controle distribuído, que se caracterizam por: meios variados de comunicação; implementação mais completa para sistemas abertos; flexibilidade completa para topologias de rede; *software* e ferramentas de desenvolvimento mais amigáveis.

Na área de instrumentação a revolução ocorreu mais lentamente. Era necessário dotar os instrumentos de mais inteligência e fazê-los se comunicar em rede. O padrão 4-20 mA para transmissão de sinais analógicos tinha que ceder lugar a transmissão digital. A princípio foi desenvolvido um protocolo (HART – *Highway Addressable Remote Transmiter*) que aproveitava o próprio cabeamento existente, fazendo transitar sinais digitais sobre sinais analógicos 4-20 mA. O HART é uma tecnologia híbrida de transição do modelo analógico para o digital, que permanece até hoje em utilização [3]. Depois surgiu uma profusão de padrões e protocolos que pretendiam ser o único e melhor barramento de campo industrial.

1.2. Revisão histórica

No final da década de 50 o uso da instrumentação pneumática já estava consolidada, quando aparecem os transmissores e controladores eletrônicos analógicos, com o padrão 4-20 mA. O novo padrão possibilitou a transmissão desse sinal a distâncias bem superiores que o sistema pneumático, permitindo o aumento na quantidade de informação vinda do processo para as salas de controle.

Nos anos 60 inicia-se o uso de computadores para o controle de processos, aparecendo o conceito do Controle Digital Direto (DDC - *Direct Digital Control*). Um único grande computador era responsável pelo controle de processo da planta [5]. O inconveniente estava na centralização de todo o cabeamento entre o campo e a sala de controle, pois cada instrumento ou equipamento precisava de um par de condutores.

No fim dos anos 60 aparece no segmento de manufatura um equipamento com a finalidade

de substituir as lógicas a relés, os controladores lógicos programáveis (CLP, ou do inglês PLC – *Programmable Logic Controller*). Concebido inicialmente para a indústria automobilística, possuía apenas entradas e saídas digitais. Com o passar do tempo passou a incorporar também entradas e saídas analógicas, passando a ser usado também na área de controle de processo.

No início dos anos 70 já estava em curso a utilização de redes de comunicação e apareciam os minicomputadores. Essas tecnologias possibilitaram o aparecimento de uma nova arquitetura para controle de processo, denominado de Sistema Digital de Controle Distribuído (DCS – *Distributed Control System*) [5]. O processamento que até então era realizado em um só computador passou a ser distribuído por computadores menores denominados de controladores.

A partir dos anos 80 aparece um novo conceito de arquitetura para controle de processo conhecido como SCADA (*Supervisory Control and Data Acquisition*). Parecido com o DCS, no que se refere à arquitetura, no lugar de controladores existem as RTUs (*Remote Terminal Units*). As RTUs são CLPs que se comunicam com os instrumentos de campo, executam os algoritmos de controle e comunicam-se com os microcomputadores. Por volta de 1980 surge também a primeira instrumentação digital [5]. Esta é caracterizada por conter um microprocessador, que lhe permitiu aumentar as potencialidades, com a capacidade de processamento local.

Mas como a transmissão de sinal continuava sendo analógica, todo esse potencial ficava limitado. A indústria já sinalizava a necessidade de utilizar um meio de comunicação digital, que permitisse o aumento do trânsito de informações do campo para a sala de controle, e vice-versa. Surge uma nova arquitetura denominada de *Fieldbus Control System* (FCS).

Devido à versatilidade, a criação de sistemas *fieldbus* tornou-se uma ocupação tendenciosa para muitas empresas de automação. Apesar dos benefícios, o número de diferentes sistemas *fieldbus* que surgiam não era bem visto pelos consumidores, acostumados com a compatibilidade presente nos sistemas já existentes, e temerosos com a possibilidade de ficarem "presos" a um único fabricante. Esta situação dificultou a disseminação dos novos conceitos [6]. Como conseqüência, organizações de usuários foram fundadas para conduzir a definição e promoção de sistemas *fieldbus*, independentemente das empresas. Surgindo assim a idéia de sistemas abertos.
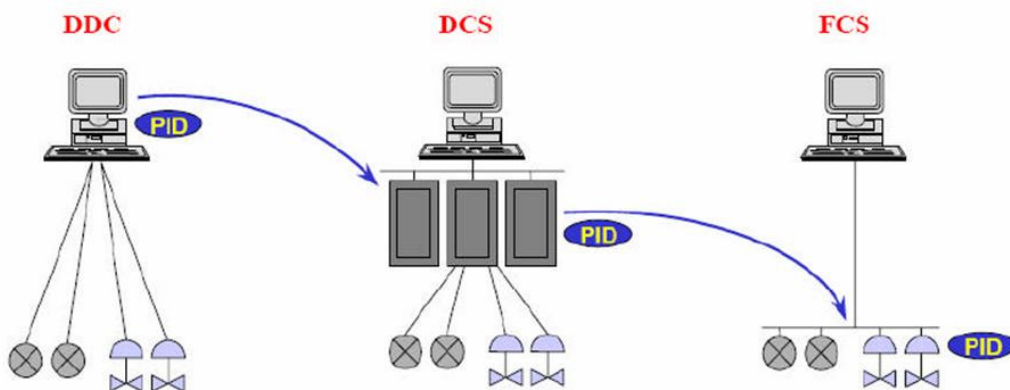
Figura 2 - A evolução do conceito de controle de processo

Em 1985, o comitê IEC SC65C iniciou o esforço de definir um padrão *fieldbus* uniforme e internacional para a automação industrial e de processos. Os dois maiores projetos de rede de campo nessa época eram o FIP (*Flux Information Processus* ou *Factory Instrumentation Protocol*) e o PROFIBUS, desenvolvidos respectivamente na França em 1982 e na Alemanha em 1984. Suas abordagens eram completamente diferentes. Um *fieldbus* universal deveria combinar os benefícios de ambos, e nos anos seguintes se viram esforços para encontrar uma convergência entre as duas abordagens.

A ISA (*Instrumentation, Systems and Automation*, que naquela época se chamava *Instrument Society of America*) e o IEC (*International Electrotechnical Comission*) decidiram juntar esforços e deste ponto em diante o trabalho técnico ficou a cargo da ISA SP50, enquanto que o IEC restringiu-se as atividades de organização dos processos de deliberação.

Devido à incapacidade dos comitês em achar uma solução, os grandes fabricantes de sistemas de automação lançaram duas iniciativas para chegar a um acordo [6]. A fundação do projeto WorldFIP, em 1993 tinha o objetivo de adicionar as funcionalidades do modelo cliente-servidor ao FIP. Por outro lado, o ISP (*Interoperable System Project*) empreendeu-se em demonstrar, a partir de 1992, como o PROFIBUS poderia ser melhorado com o modelo *publisher-subscriber* semelhante ao encontrado no FIP.

Com o fim do projeto ISP, por questões estratégicas, muitos de seus antigos membros juntaram forças com integrantes do WorldFIP norte-americano e formaram a Fieldbus Foundation. Esta nova associação iniciou a definição de uma nova rede de campo para processos industriais: a FOUNDATION Fieldbus. Enquanto a discussão sobre a padronização acontecia, os sistemas *fieldbus* atacaram o mercado, investindo em desenvolvimento de protocolos e equipamentos, e já existiam muitas instalações em funcionamento. Os comitês nacionais na Europa, após longas discussões, chegaram a um acordo sem precedentes: todos os padrões nacionais seriam considerados padrões europeus. Enquanto isso, a Fieldbus Foundation preparava sua própria especificação. Esse trabalho acabou influenciando no comitê do IEC, e para vários de seus membros isto parecia ser o fim de um longo debate. Contudo, o projeto não foi aprovado em votação. Como, de acordo com as regras de padronização européias, seguindo o Acordo de Dresden (*Dresden Agreement*, tratado firmado entre o IEC e o CENELEC), um padrão internacional se sobrepõe, os defensores do PROFIBUS temiam que o FOUNDATION Fieldbus obtivesse vantagem competitiva e que o PROFIBUS perdesse terreno [6]. Dessa forma, os países onde o PROFIBUS dominava organizaram-se para impedir a aprovação do padrão.

Em julho de 1999, representantes dos principais adversários envolvidos na questão (Fieldbus Foundation, Fisher Rosemount, ControlNet International, Rockwell Automation, Profibus User Organization e Siemens) assinaram um "memorando de entendimento" com o intuito de

terminar a guerra em torno do padrão *fieldbus*. A idéia era criar um padrão abrangente, acomodando todos os sistemas *fieldbus*. Finalmente, o padrão de rede de campo internacional, IEC 61158, foi lançado em 31 de dezembro de 2000. Este padrão contém uma coleção de módulos de especificação úteis para a implementação de *fieldbuses*, de acordo com o observado na Tabela 1.

Tabela 1 - Padrão IEC 61158

Documentos IEC 61158	**Conteúdo**
61158-1	Introdução
61158-2	Especificação da camada física
61158-3	Definição dos serviços da camada de enlace
61158-4	Especificação dos protocolos da camada de enlace
61158-5	Definição dos serviços da camada de aplicação
61158-6	Especificação dos protocolos da camada de aplicação

Simultaneamente ao desenvolvimento das redes *fieldbus*, as técnicas de comunicação também sofreram modificações. Diversos são os meios de transmissão disponíveis atualmente: fios, cabos, fibras óticas e ondas eletromagnéticas. Inúmeros também são os protocolos e padrões usados para suprir as exigências destes meios por onde trafegam os dados. As tecnologias de comunicação industrial acompanham tais evoluções, incorporando-as, e sempre visando a melhor solução para os problemas existentes.

2. Redes industriais *fieldbus*

As redes de campo são redes locais de comunicação, bidirecionais, projetadas e utilizadas para interligar entre si instrumentação industrial de medida, dispositivos de controle e sistemas de operação industriais [5].

Eis a definição de redes *fieldbus* dada pelo IEC 61158: "Uma rede de campo é um barramento de dados digital, serial, *multidrop*, para comunicação com dispositivos de controle e dispositivos de instrumentação tais como transdutores, atuadores e controladores locais, não sendo restrito a estes".

Os sistemas *fieldbus* estão presentes em todos os domínios da automação: controle de processo, automação residencial, construção de máquinas, aplicações ferroviárias e automotivas, e aviação.

Alguns barramentos servem apenas para interligar sensores e atuadores discretos, basicamente transmitindo estados e *bits* de comando, necessitando de processamento mínimo por parte do instrumento. São as redes de nível mais baixo, denominadas de *Sensorbus*. Um segundo nível é representado pelas redes capazes de interligar dispositivos mais inteligentes, enquadradas na denominação genérica de *Devicebus*. As mensagens aqui já são orientadas a *bytes*. Finalmente restam as redes de instrumentos de campo, ou *Fieldbus*, especializadas em variáveis de controle. Suportam uma maior transmissão de dados, e necessitam de maior poder de processamento por parte dos dispositivos. Uma ilustração dessa classificação é apresentada na Figura 3.
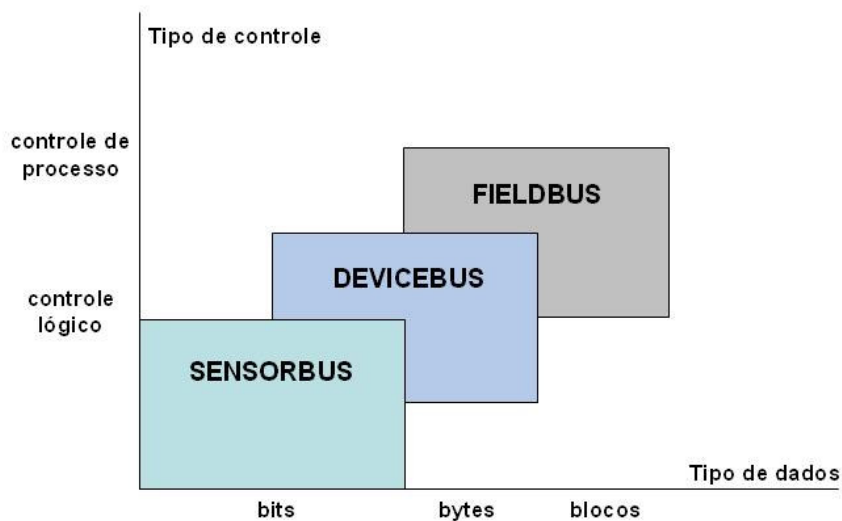
Figura 3 - Classificação das redes de campo industriais

Os protocolos *fieldbus* são modelados de acordo com o modelo OSI/ISO. Entretanto, apenas as camadas 1, 2 e 7 são usadas. Assim, o padrão IEC 61158 descreve uma estrutura em três camadas, formada pelas camadas física, de enlace e de aplicação. As funções das camadas 3 e 4

podem ser alocadas nas camadas 2 ou 7, já as funções das camadas 5 e 6 são cobertas pela camada de aplicação.

As redes de campo são tipicamente redes de um único segmento, e as extensões são feitas através de repetidores, ou no máximo *bridges* (pontes).

A coleção de módulos de especificações de redes de campo do padrão IEC 61158 era útil para qualquer implementação prática. O que faltava era um manual de utilização, mostrando que partes podem ser reunidas em um sistema funcional e como isto pode ser efetuado. Este guia veio com o IEC 61784-1 como uma definição dos então chamados perfis de comunicação. Os perfis podem ser vistos como uma camada adicional no topo do modelo OSI, sendo conhecida como camada de usuário.

Vantagens das redes de automação em relação a sistemas convencionais de cabeamento:

- Expansão da rede com o sistema em funcionamento;
- Redução de materiais (cabos, painéis, caixas de junção, etc.);
- Interoperabilidade entre equipamentos de fabricantes distintos;
- Atualização de *firmware* a partir da sala de controle;
- Capacidade de auto-reconhecimento do instrumento;
- Facilidade na manutenção;
- Flexibilidade na configuração da rede;
- Possibilidade de diagnósticos dos dispositivos.

Por usarem protocolos de comunicação padronizados possibilitam a integração de equipamentos de vários fabricantes distintos, tais sistemas dizem-se abertos, são flexíveis e têm capacidade de expansão.

São vários os padrões de redes industriais de comunicação empregados na indústria. Recentemente as redes PROFIBUS e FOUNDATION Fieldbus apresentaram um grande crescimento no número de instalações na indústria de processos, como o setor petroquímico, sendo líderes dos investimentos no ramo dos sistemas *fieldbus* [40]. A Tabela 2 contém os dados de um estudo realizado pela ARC Advisory Group, contendo os valores obtidos em 2006 e uma estimativa para o ano de 2011.

Tabela 2 - Investimentos em *fieldbus* nas indústrias de processo, em milhões de dólares.

	Rendimentos em 2006	**Rendimento em 2011**	**TCAC***
FOUNDATION Fieldbus	566,6 (68,1%)	1.714,2 (75,2%)	24,8%
PROFIBUS	263,8 (31,7%)	564,1 (24,7%)	16,4%
Outros	1,3 (0,2%)	1,5 (0,1%)	3,6%
TOTAL	831,7 (100%)	2.279,8 (100%)	22,3%

* Taxa de crescimento anual composta

Fonte: ARC Advisory Group, 2007

O aumento no número de usuários e a previsão de crescimento para os próximos anos, foram os principais pontos na escolha das redes PROFIBUS e FOUNDATION Fieldbus como objetos dos estudos deste trabalho. As seções a seguir expõem as características dessas duas redes industriais de comunicação.

2.1. PROFIBUS

O PROFIBUS é baseado no modelo OSI/ISO, conforme apresentado na Figura 4. A camada 1 (nível físico) define as características físicas de transmissão, a camada 2 (enlace de dados) define o protocolo de acesso ao meio e a camada 7 (aplicação) define as funções de aplicação. Além destas camadas há também a presença da camada de usuário.
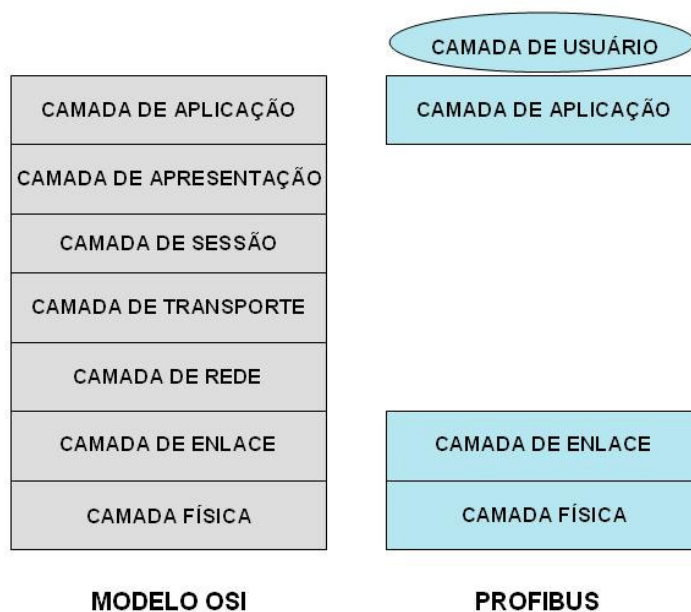
Figura 4 - As camadas do PROFIBUS

A aplicação de um sistema de comunicação industrial é amplamente influenciada pela escolha do meio de transmissão. Requisitos de uso genérico, como alta confiabilidade, grandes distâncias cobertas e alta velocidade de transmissão, somam-se as exigências específicas da área de automação de processos tais como operação em áreas classificadas, transmissão de dados e alimentação no mesmo meio físico, etc. Existem atualmente três tipos físicos disponíveis no PROFIBUS [12]:

- RS485: para uso universal;
- IEC 61158-2: para aplicações em sistemas de automação de controle de processos;
- Fibra ótica: para aplicações em sistemas que demandam grande imunidade às interferências eletromagnéticas e grandes distâncias.

O padrão RS485 é a tecnologia de transmissão mais encontrada no PROFIBUS. É simples, de baixo custo, primordialmente usada para tarefas que requerem altas taxas de transmissão [12].

Um cabo de cobre blindado com um par de condutores em par trançado (STP – *shield twisted pair*) é usado. A estrutura do barramento permite a adição ou remoção de estações sem interferir nas demais. Possíveis expansões não têm efeito sobre as estações em operação. É possível selecionar taxas de transmissão desde 9,6 kbps até 12 Mbps, porém uma única taxa é selecionada para todos os dispositivos no barramento quando o sistema é inicializado. Até 32 estações podem ser conectadas em um único segmento. Para conectar mais do que 32 estações, ou no caso que a distância total entre as estações ultrapasse um determinado limite, devem ser utilizados repetidores para interconectar diferentes segmentos do barramento. O comprimento máximo da linha depende da taxa de transmissão. O barramento é encerrado por um terminador ativo do barramento, no início e no fim de cada segmento.

A transmissão síncrona em conformidade com a norma IEC 61158-2 veio atender aos requisitos das indústrias químicas e petroquímicas. Permite, além de segurança intrínseca, que os dispositivos de campo sejam energizados pelo próprio barramento. Os dispositivos de campo agem como consumidores passivos de corrente. Uma terminação passiva de linha é necessária, em ambos os fins da linha principal do barramento. Topologia linear, árvore e estrela são permitidas [12]. É uma transmissão síncrona, na codificação *Manchester*, com taxa de transmissão de 31,25 kbps usando tecnologia a dois fios. É usualmente limitada a um determinado segmento da planta, por exemplo, dispositivos de campo em áreas perigosas. Da mesma forma que no padrão RS485, também são possíveis até 32 estações por segmento [7].

Fibras óticas são usadas para aplicações *fieldbus* que tenham alta interferência eletromagnética, ou que cubram uma grande área ou distância. O PROFIBUS inclui fibras multimodo e monomodo de vidro, fibras de plástico, entre outras [7].

Na sala de controle estão localizados o sistema de controle de processo e os dispositivos de monitoração e operação, interconectados por RS485. No campo, dispositivos do tipo *Coupler* ou *Link* adaptam os sinais do segmento RS485 aos sinais do segmento IEC 61158-2. Do ponto de vista do protocolo, os dispositivos *Couplers* são transparentes. Se estes são usados, a velocidade do segmento RS485 ficará limitada em no máximo 45,45 kbps ou 93,75 kbps. Os *Links*, por sua vez, possuem sua própria inteligência intrínseca. Eles tornam todos os dispositivos conectados ao segmento IEC 61158-2 um único dispositivo escravo no segmento RS485. Neste caso não há limitação de velocidade no segmento RS485, além do aumento na capacidade de endereçamento. Ambos os tipos de dispositivo possuem o terminador de barramento integrado.

Perfis são usados em automação para definir comportamentos e propriedades específicas de dispositivos, família de dispositivos ou sistemas inteiros. O termo perfil engloba desde poucas especificações de uma classe de dispositivos, até especificações abrangentes de aplicações em uma determinada indústria [7].

O perfil de aplicação define as opções de protocolo e da tecnologia de transmissão requerida

nas respectivas áreas de aplicação e para os vários tipos de dispositivos. Estes perfis também definem o comportamento do dispositivo.

Os perfis de comunicação PROFIBUS usam um protocolo uniforme de acesso ao meio, implementado pela camada de enlace de dados do modelo OSI/ISO. No PROFIBUS, a camada 2 é chamada *Fieldbus Data Link* (FDL). O controle de acesso ao meio (MAC) especifica o procedimento quando uma estação tem a permissão para transmitir, além de assegurar que uma única estação tem direito de transmitir neste momento. A detecção de defeitos no meio de transmissão ou no receptor, assim como detecção de erros de endereçamento ou na passagem do *token* são funções do MAC no PROFIBUS.

No nível de campo, a periferia distribuída, dispositivos tais como módulos de E/S, transdutores, acionamentos, válvulas e painéis de operação, se comunicam com sistemas de automação via um eficiente sistema de comunicação em tempo real, o PROFIBUS-DP ou PROFIBUS-PA. A transmissão de dados é efetuada ciclicamente, enquanto alarmes, parâmetros e diagnósticos são transmitidos aciclicamente, só quando necessário [7].

O PROFIBUS diferencia seus dispositivos entre mestres e escravos. Os mestres determinam a comunicação de dados no barramento. O protocolo PROFIBUS de acesso ao barramento inclui o procedimento de passagem de *token*, usado pelos mestres para comunicar-se uns com os outros, e o procedimento mestre-escravo, usado pelos mestres para se comunicarem com seus escravos. O *token* é passado de um mestre ao próximo em ordem crescente de endereços. No momento que uma estação ativa recebe o *token*, passa a executar seu papel de mestre durante um período determinado, podendo se comunicar com todas as estações escravas num relacionamento mestre-escravo, e com todas as estações mestre num relacionamento mestre-mestre de comunicação. Esse modo de comunicação é ilustrado na Figura 5.
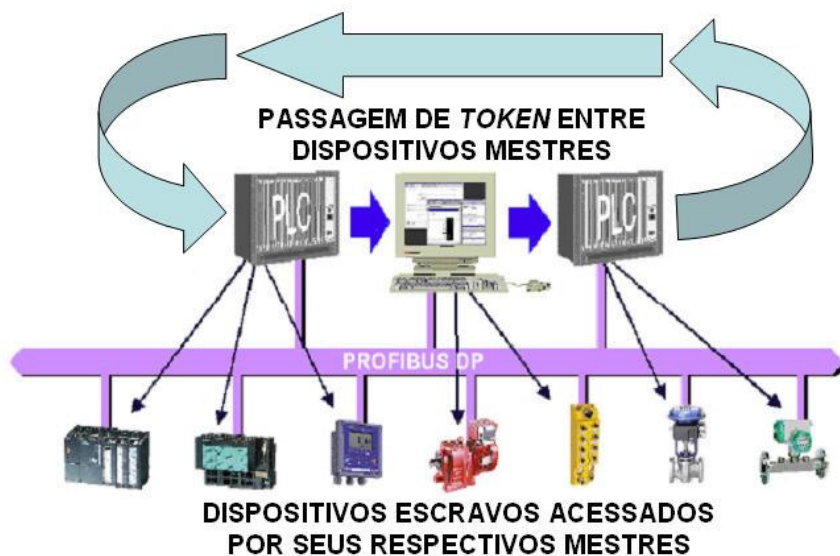
Figura 5 - Mecanismo de comunicação no PROFIBUS

A camada FDL opera no modo sem conexão. Além de transmissão ponto a ponto, proporciona também comunicações do tipo multiponto (*broadcast* e *multicast*).

Cada perfil de comunicação PROFIBUS usa um subconjunto específico dos serviços da camada FDL. Os serviços são acionados por camadas superiores via pontos de acesso de serviço (SAPs – *service acess points*) [12].

Dispositivos PROFIBUS possuem diferentes características de funcionalidade ou de parametrização da comunicação. Estes parâmetros variam para cada tipo de dispositivo e de fabricante. A fim de tornar o PROFIBUS um sistema facilmente configurável, tipo *plug and play*, definiu-se um arquivo de dados eletrônico do dispositivo (arquivo GSD), onde estas informações são armazenadas. Os arquivos GSD ampliam a característica de rede aberta, podendo ser carregado durante a configuração, tornando a integração de dispositivos de diversos fabricantes em um sistema PROFIBUS simples e amigável. Os arquivos GSD fornecem uma descrição clara e precisa das características de um dispositivo em um formato padronizado. O arquivo GSD é dividido em três seções:

- Especificações gerais: informações sobre fabricante, nome do dispositivo, revisão de hardware e software, taxas de transmissão suportadas e possibilidade para a definição do intervalo de tempo para monitoração;
- Especificações relacionadas ao mestre: parâmetros relacionados ao mestre, tais como número máximo de escravos ou opções de *upload* e *download*. Exclusivo para dispositivos mestres;
- Especificações relacionadas ao escravo: especificações tais como número e tipo de canais de I/O, especificação de informações de diagnósticos, etc.

Uma distinção é feita entre parâmetros obrigatórios e parâmetros opcionais. O formato dos arquivos GSD contém listas (tal como velocidade de comunicação suportada), assim como espaços para descrever os tipos de módulos disponíveis em um dispositivo modular [12].

2.1.1. PROFIBUS DP

No PROFIBUS-DP, os controladores centrais se comunicam com seus dispositivos de campo distribuídos via um *link* serial de alta velocidade [12]. A maior parte desta comunicação é feita de uma maneira cíclica. Funções de comunicação não cíclicas estão disponíveis para dispositivos de campo inteligentes, permitindo assim configuração, diagnóstico e manipulação de alarmes.

O PROFIBUS-DP usa as camadas 1 e 2, bem como a interface de usuário. As camadas 3 a 7 não são usadas.

A principal tecnologia usada pelo PROFIBUS-DP na camada física é o padrão RS485, sendo possível utilizar fibras óticas, caso haja necessidade.

O PROFIBUS-DP difere três grupos de dispositivos no barramento. O DPM1 (DP *master class* 1) é um controlador central que ciclicamente troca informações com as estações (escravos) em um ciclo de mensagem específico. Dispositivos típicos são CLPs e PCs. DPM2 (DP *master class* 2) consiste em terminais de engenharia, programadores, dispositivos de configuração ou painéis de operação. Usados durante o comissionamento para configuração do sistema DP e também para a manutenção e diagnóstico do barramento e/ou de seus dispositivos. Não precisam estar conectados permanentemente ao barramento. Os escravos DP (DP *slaves*) são periféricos (acionamentos, válvulas, atuadores, sensores, etc.). São dispositivos passivos: só respondem a requisições diretas.

PROFIBUS-DP suporta a implementação de sistemas monomestre e multimestre. Um máximo de 126 dispositivos (mestres ou escravos) pode ser conectado ao barramento da rede. São reservados oito *bits* para o campo de endereço, porém apenas sete são efetivamente usados para endereços: o *bit* mais significativo do *byte* indica a utilização dos campos de ponto de acesso de serviço. Em sistemas monomestre, apenas um mestre está ativo no barramento. Em sistemas multimestre diversos mestres compartilham o mesmo barramento. Eles representam subsistemas independentes, englobando mestre e seus respectivos escravos. A coordenação dos mestres é feita por passagem de *token*, apenas o mestre que detém o *token* pode comunicar.

A imagem de entrada e saída dos escravos DP pode ser lida por todos os mestres DP. Entretanto, somente um único mestre poderá escrever em uma saída. Naturalmente, sistemas multimestre possuem um tempo de ciclo mais longo que sistemas monomestre [12].

Durante a configuração do sistema, o usuário especifica a associação de um escravo DP ao DPM1 e quais escravos DP serão incluídos ou excluídos da transmissão cíclica de dados do usuário. A transmissão de dados entre o DPM1 e os escravos DP é dividida em três fases: parametrização, configuração e transferência de dados. Durante as fases de parametrização e configuração de um escravo DP, sua configuração real é comparada com a configuração projetada no DPM1, somente se corresponderem é que o escravo DP passará para a fase de transmissão de dados. Assim, todos os parâmetros de configuração, tais como tipo de dispositivo, formato e comprimento de dados, número de entradas e saídas, etc. devem corresponder à configuração real. Uma nova parametrização pode ser enviada ao escravo DP sempre que necessário [12].

O PROFIBUS-DP foi projetado para troca rápida de dados em nível de campo. Está disponível em três versões: DP-V0, DP-V1 e DP-V2, cada uma com características próprias.

A versão DP-V0 provê funcionalidades básicas do DP, incluindo troca cíclica de dados bem como diagnóstico de estações, de módulos, e específicas de um canal. O mestre lê ciclicamente a informação dos escravos e escreve também ciclicamente a informação nos escravos. Comunicação cíclica entre o DPM1 e seus escravos é feita em uma seqüência recorrente e definida. O usuário define os escravos de cada DPM1 na configuração do sistema. Além dessa comunicação personalizada (direcionada a um escravo) o mestre pode enviar comandos de controle a todos os

escravos, ou a um grupo, simultaneamente. Esses comandos são transmitidos como mensagens *broadcast* ou *multicast*.

A versão DP-V1 contém melhorias montadas para a automação de processos, em particular comunicação acíclica de dados, ponto chave dessa versão [7], para indicação de parâmetros e calibração dos dispositivos de campo ao longo do barramento durante a operação; visualização, operação e manipulação de alarmes de dispositivos inteligentes. A transmissão acíclica é feita em paralelo à transmissão cíclica de dados de usuário, mas com baixa prioridade.

A versão DP-V2 contém ainda mais melhorias e é montada primordialmente para as demandas da tecnologia de acionamentos. A comunicação escravo-escravo permite comunicação direta entre escravos, usando *broadcast*. Os dados não passam pelo mestre, vão diretamente a outros escravos, permitindo que escravos leiam dados de outros escravos e usem esses dados como entradas. Isto abre a possibilidade de novas aplicações, e reduz o tempo de resposta no barramento em até 90% [7].

A quantidade de informação de I/O depende do tipo de dispositivo. Um máximo de 246 *bytes* de entrada e 246 *bytes* de saída é permitido. O PROFIBUS-DP requer aproximadamente 1 ms, à 12 Mbps, para a transmissão de 512 *bits* de dados de entrada e 512 *bits* de dados de saída distribuídos em 32 estações [12]. A estrutura dos quadros da camada de enlace e da camada física é mostrada na Figura 6.
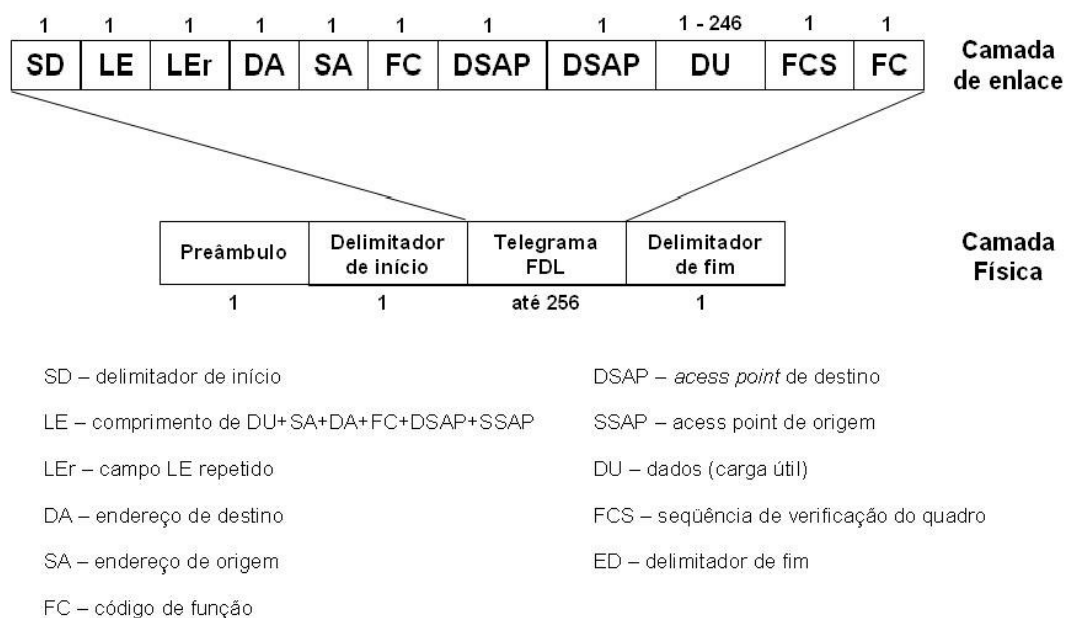
Figura 6 - Estrutura de quadros nas camada de física e de enlace do PROFIBUS

Uma proteção contra erros do equipamento de transmissão é conseguida no PROFIBUS DP com um mecanismo de monitoração de tempo, implementado tanto no mestre quanto nos escravos. O DPM1 monitora a transmissão de dados dos escravos com o *Data_Control_Timer*, um temporizador de controle independente para cada escravo. O temporizador expira se uma correta

transmissão de dados não ocorrer dentro do intervalo de monitoração. O escravo usa o controle *watchdog* para detectar falha no mestre ou na linha de transmissão. Se nenhuma comunicação com o mestre ocorre dentro do intervalo do *watchdog*, o escravo automaticamente muda suas saídas para o estado de segurança (*fail-safe*) [12].

2.1.2. PROFIBUS PA

O uso do PROFIBUS em dispositivos e aplicações típicas de automação e controle de processos é definido pelo perfil PA. A camada física utiliza o padrão IEC 61158-2. O perfil dos dispositivos PA define todas as funções e parâmetros para diferentes classes de dispositivos para automação de processos com inteligência local. O perfil é documentado em uma descrição de modelo geral contendo as especificações atualmente válidas para todos os tipos de dispositivos, e em um *data sheet* de dispositivo com especificações adicionais para classes de dispositivos individuais [7].

O perfil de aplicação PA é baseado no perfil de comunicação DP, especificamente na versão DP-V1. Os valores e o estado dos dispositivos de campo PA são transmitidos ciclicamente com alta prioridade entre um DPM1 e os escravos usando as rápidas funções básicas do DP. Por outro lado, os parâmetros do dispositivo para visualização, operação, manutenção e diagnóstico são transmitidos pelos terminais de engenharia (DPM2) com as funções DP acíclicas de baixa prioridade.

A especificação para dispositivos PA usa o modelo de blocos de função para representar seqüências funcionais [7, 12]. Uma aplicação é composta de vários blocos de função. Os blocos são integrados nos dispositivos de campo e podem ser acessados via comunicação, assim como pelo terminal de engenharia. São usados três tipos de blocos:

- Bloco físico: contém os dados característicos do dispositivo, como nome, fabricante, versão, número de série, etc. Só pode haver um bloco físico em cada dispositivo;
- Bloco transdutor: contém os dados necessários ao processamento dos sinais entregues pelo sensor. Se nenhum processamento é requerido, esse bloco pode ser omitido. O número de blocos é correspondente ao número de sensores presentes no dispositivo;
- Bloco de função: contém todos os dados para o processamento final do valor medido antes da transmissão ao sistema de controle.

O acoplamento entre segmentos DP e PA é realizado por dispositivos *Couplers* ou *Links*, como descrito na seção 2.1.1. Os *Links* DP/PA possuem a vantagem de aumentarem a capacidade de endereçamento da rede e não limitarem a velocidade no segmento DP, conforme está ilustrado na Figura 7.
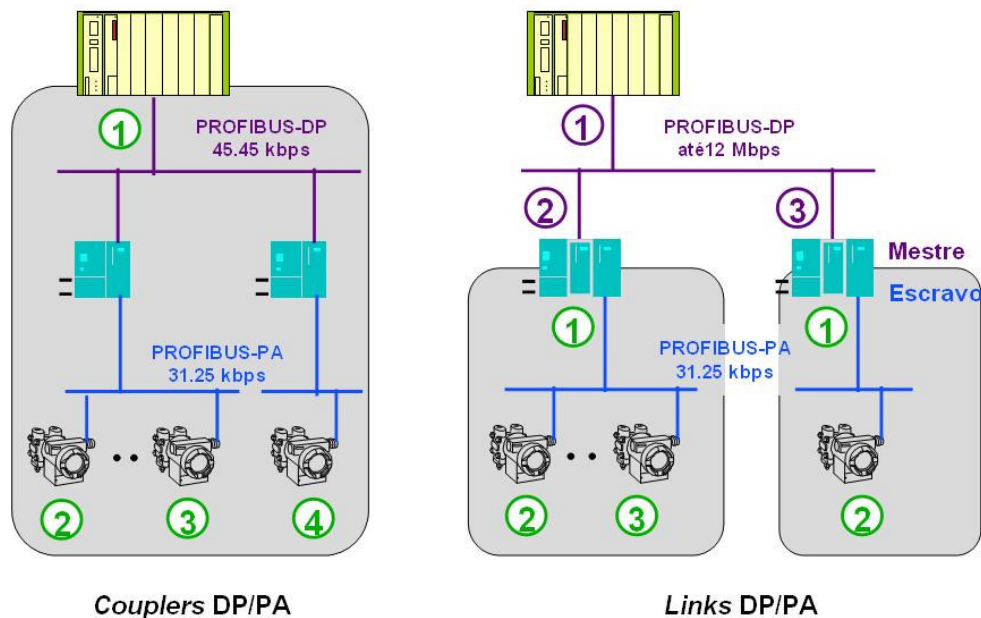
Figura 7 - Comparativo entre o uso de *Couplers* e *Links* no acoplamento de segmentos PROFIBUS DP e PA

2.1.3. PROFIBUS FMS

O perfil de comunicação FMS foi projetado para a comunicação no nível de células. Neste nível, controladores (CLPs e PCs) comunicam-se uns com outros.

No PROFIBUS-FMS as camadas 1, 2 e 7 são essenciais. A camada de aplicação é composta do FMS (*fieldbus message specification*) e do LLI (*lower link interface*). O FMS define uma ampla seleção de serviços de comunicação mestre-mestre ou mestre-escravo. O LLI define a representação destes serviços FMS no protocolo de transmissão de dados.

A parte da aplicação situada no dispositivo de campo que pode ser acessada via comunicação é denominada de dispositivo virtual de campo (VFD – *virtual field device*).

Todos os objetos de comunicação de um dispositivo FMS são registrados em um dicionário de objetos. O dicionário contém a descrição, estrutura e tipo de dados, assim como a associação entre os endereços internos e sua denominação no barramento. Os objetos podem ter um endereçamento lógico ou serem endereçados pelo nome. Também podem ser protegidos do acesso não autorizado, ou os serviços de acesso é que podem ser restringidos (ex.: só leitura) [12].

Serviços PROFIBUS-FMS disponíveis: gerenciamento de contexto (estabelecer ou encerrar conexões lógicas); acesso a variáveis; gerenciamento do domínio (transmitir grande quantidade de memória); gerenciamento de chamada de programas; gerenciamento de eventos (transmitir mensagens de alarmes); suporte VFD (identificação e status); gerenciamento de dicionário de objetos (leitura e escrita no dicionário).

O mapeamento das camadas 2 a 7 é gerenciado pelo LLI, que executa controle de fluxo e monitoração da conexão. O LLI provê vários tipos de associação de comunicação para a execução

do FMS e serviços de gerenciamento. As associações de comunicação orientada à conexão representam uma conexão lógica ponto a ponto entre dois processos de aplicação. As associações de comunicação sem conexão possibilitam a um dispositivo se comunicar simultaneamente com diversas estações usando serviços não-confirmados [12].

2.1.4. PROFINET

PROFINET fornece uma comunicação baseada na Ethernet capaz de combinar os benefícios da comunicação corporativa (TCP/IP, HTTP, SMTP, etc.) com os requisitos da comunicação industrial. Provê acesso direto do nível corporativo para o nível de automação, e vice-versa.

PROFINET pode atuar como um "*backbone*" para interligar sub-redes PROFIBUS DP e PA. A integração de segmentos PROFIBUS no PROFINET é realizada usando-se *gateways*. O conceito de *proxy* também é usado na tarefa de conversão entre os dois sistemas de comunicação, sendo parte da integração. Isto resulta na utilização da tecnologia de transmissão PROFIBUS, especificamente desenvolvida para automação, sem precisar sacrificar os benefícios da tecnologia PROFINET.
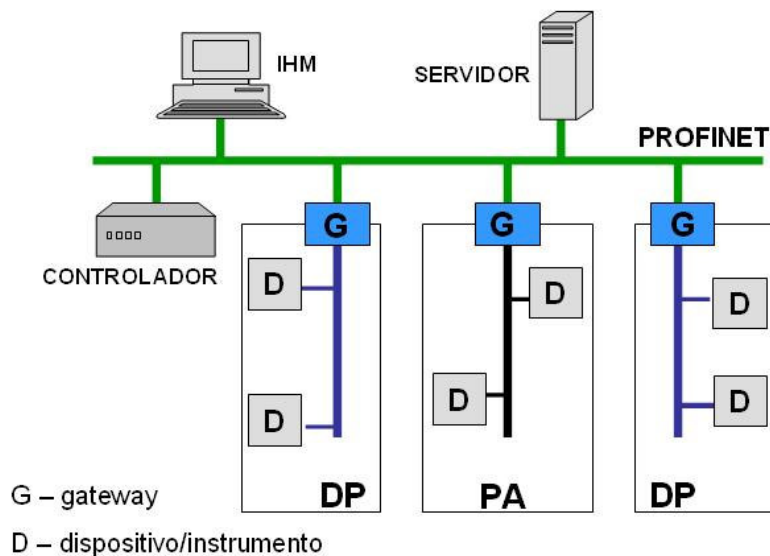
Figura 8 - Exemplo do uso de PROFINET numa planta industrial

2.2. FOUNDATION Fieldbus

Deve-se tomar cuidado para não confundir o nome da rede FOUNDATION Fieldbus com o da fundação que a criou e a mantém, esta sim denominada Fieldbus Foundation.

Os princípios básicos definidos no surgimento do FOUNDATION Fieldbus incluem duas pedras fundamentais: a adoção dos dois principais mecanismos de acesso ao meio, e a ênfase em uma descrição padronizada dos dispositivos [8].

Circulação de *token* e acesso agendado eram bons, mas insuficientes; sendo complementares. A Fieldbus Foundation adotou uma abordagem para dispor tanto da filosofia programada do FIP, quanto da filosofia de rotação de *token* do PROFIBUS.

A ênfase em uma descrição padronizada permitiu evitar a situação na qual, após definir a pilha de comunicação, muito ainda precisaria ser feito para tornar os dispositivos operacionais após conectá-los ao barramento. FOUNDATION Fieldbus tinha esse conceito em mente desde o começo e incluiu a definição das semânticas dos dados mais suas configurações, e usou dentro do primeiro conjunto de especificações [8].

As especificações FOUNDATION Fieldbus incluem duas diferentes configurações: H1 e HSE. A configuração H1 interconecta equipamentos de campo como sensores, atuadores e I/Os, e funciona a 31,25 kbps. HSE provê integração dos controladores (como sistemas de controle distribuídos e CLPs), dos subsistemas H1, dos servidores de dados e estações de trabalho, e funciona à 100 Mbps. Um exemplo de uso do FOUNDATION Fieldbus em uma planta industrial é apresentado na Figura 9.
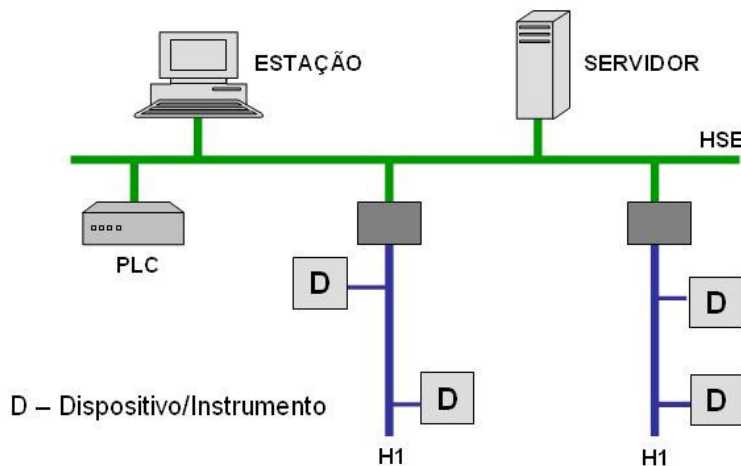
Figura 9 - Rede FOUNDATION Fieldbus em plantas industriais

Tanto o H1 quanto o HSE possuem uma camada de aplicação de usuário, que é baseada em blocos representando os diferentes tipos de aplicações. Os tipos de blocos são: recursos, transdutor e funções.

O bloco de recursos descreve características do dispositivo de campo, tais como nome, fabricante e número de série. Há apenas um bloco de recurso por dispositivo.

Os blocos de transdutor são usados para configurar os dispositivos de campo. Eles desacoplam os blocos de funções das funcionalidades de entrada/saída locais exigidas na leitura de sensores ou comando de atuadores [8]. Eles contêm informação como dados de calibração e tipo de sensor. Normalmente há um transdutor para cada entrada e saída do bloco [16].

Os blocos de função provêm o controle e comportamento do sistema. São funções de automação padronizadas. Os parâmetros de entrada e saída dos blocos de função podem ser ligados

diretamente no barramento. A execução de cada bloco de função é precisamente agendada. Pode haver muitos blocos de função em uma única aplicação de usuário [16]. A Fieldbus Foundation definiu um conjunto de blocos de função padrão que podem ser combinados e parametrizados para criar um dispositivo. Os blocos de função podem ser construídos em dispositivos para alcançar a funcionalidade desejada.

A solução é o uso de uma linguagem descritiva de dispositivos, a DDL (*device description language*). Ela é capaz de descrever formalmente o dispositivo e pode ser interpretada pela biblioteca de serviços de descrição de dispositivos disponível no FOUNDATION Fieldbus. Tal descrição age como um *driver* para cada dispositivo. Dentro de cada descrição, e para cada bloco de função no dispositivo, uma hierarquia é seguida: (1) parâmetros universais do dispositivo; (2) parâmetros comuns a cada bloco e função; (3) parâmetros comuns aos blocos transdutores; e (4) parâmetros específicos do fabricante. As descrições também podem incluir pequenos programas para interação com o dispositivo (por exemplo, para calibração), assim como capacidade de carregar atualizações [8].

2.2.1. FOUNDATION Fieldbus H1

No sistema de comunicação FOUNDATION Fieldbus H1, suas funcionalidades são suportadas por serviços agrupados em níveis, assim como outras arquiteturas baseadas no modelo OSI/ISO. Abaixo da camada de aplicação, há a camada de enlace de dados, que lida com o acesso ao canal de comunicação. A camada física lida com a interface com o meio físico.

A camada física do H1 foi concebida para receber as mensagens da pilha de comunicação e convertê-las em sinais físicos no meio de transmissão *fieldbus*, e vice-versa. As tarefas de conversão incluem a adição e remoção de preâmbulos e delimitadores de início e fim [8]. O preâmbulo é usado pelo receptor para sincronizar seu *clock* interno com o sinal vindo do barramento. Os delimitadores são usados para identificar o início e fim dos dados.

O objetivo era substituir os dispositivos 4-20 mA existentes, na tentativa de reduzir custos. Essa mudança seria mais fácil se o cabeamento existente, que suportava apenas a versão H1 de baixa velocidade, fosse mantido [8].

Sinais (± 10 mA com 50 Ω de carga) são codificados usando a técnica Manchester síncrona, e podem ser conduzidos em cabos de par trançado. O sinal é chamado serial síncrono porque a informação de *clock* está embutida na seqüência de dados serial. O receptor interpreta uma transição positiva no meio do período de *bit* como um 0 lógico e uma transição negativa como um 1 lógico. Um exemplo da transmissão de uma seqüência de bits usando essa codificação pode ser visto na Figura 10. O transmissor entrega ± 10 mA à 31,25 kbps com uma impedância de 50 Ω para criar uma tensão de 1 V pico a pico modulada na tensão de alimentação DC, que pode ser de 9 a 32 volts.
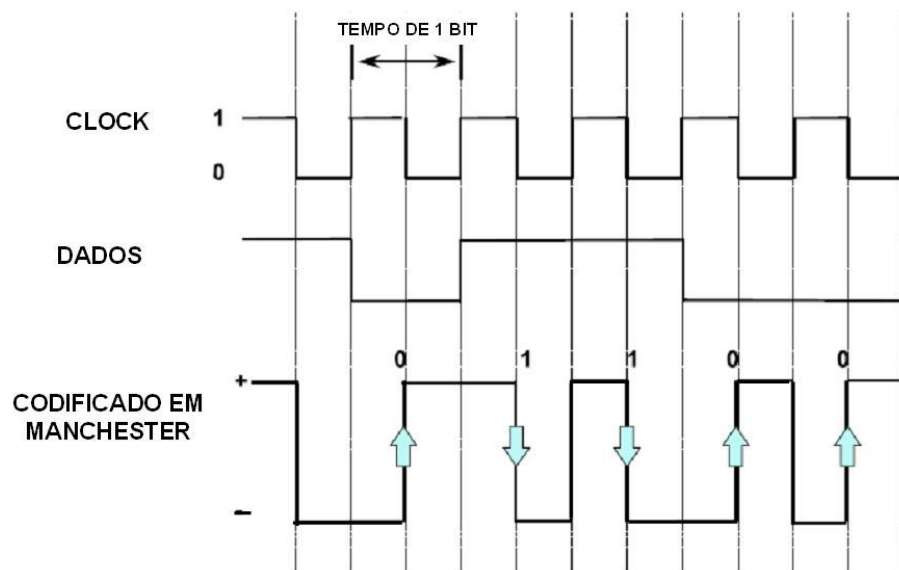
Figura 10 - Codificação Manchester

A fiação H1 é baseada em cabos-troncos com terminadores em cada ponta. Cada cabo é encerrado com um terminador de 100 Ω de impedância. Isto faz do cabo de instrumentação uma linha de transmissão balanceada em que um sinal de freqüência relativamente alta pode ser transmitido com um mínimo de distorção [18].

Permite derivações localizadas em qualquer ponto ao longo do tronco e conectadas por meio de caixas de junção. Um único dispositivo pode ser conectado em cada derivação. Outros troncos podem ser encadeados através de repetidores. Até cinco troncos podem ser interconectados. O comprimento de uma derivação varia de 1 a 120 m, dependendo do número de dispositivos conectados ao enlace *fieldbus*. O número máximo de dispositivos em um tronco H1 é 32, porém o número real depende de fatores como consumo de potência, tipo de cabo, repetidores, etc. O comprimento total do tronco, incluindo as derivações pode ser até 1900 m, e 240 é o número de endereços de rede disponíveis [7].

A camada de enlace do FOUNDATION Fieldbus H1 controla a transmissão de mensagens no barramento. Um agendamento completo capaz de garantir os dados necessários em tempo hábil, mas também permitindo lacunas, nas quais um mecanismo de *token* assume obedecendo a um tempo máximo de rotação definido. Para tanto é preciso um mediador que impõe a transmissão de dados por uma determinada entidade em tempos definidos quando requerido, mas também garante uma quantidade definida de tempo livre para cada entidade. Este mediador é o LAS (*link active scheduler*). Essencialmente o LAS executa:

- Acesso ao meio físico com base numa programação;
- Circulação de *token* apenas quando nenhum tráfego agendado é necessário. O *token* é passado por um período de tempo limitado que é sempre menor que o intervalo restante para o próximo tráfego agendado;

- Uma política de gerenciamento do *token*, de maneira que o *token* retorna ao LAS ao invés de seguir para o próximo nó, para que assim o LAS possa decidir, dependendo do tempo restante, se passa o *token* mais uma vez ou retorna o controle do enlace ao tráfego agendado.

Dois tipos de dispositivos são definidos nas especificações da camada de enlace H1: básico e mestre de enlace. Os básicos não têm capacidade de se tornarem o LAS. Como um barramento pode ter múltiplos dispositivos do tipo mestre de enlace, se o atual LAS falhar um destes pode se tornar o LAS e a operação do barramento pode continuar.

A comunicação agendada ocorre da seguinte forma: o LAS tem uma lista com os tempos de transmissão de todos os *buffers* de dados, em todos os dispositivos, que precisam ser transmitidos ciclicamente. Quando é tempo de um dispositivo enviar o conteúdo de um *buffer*, o LAS emite uma mensagem para compelir os dados (CD – *compel data*) ao dispositivo. Ao receber a mensagem CD, o dispositivo divulga (ou publica) o *data item* (DT) do *buffer* para todos os dispositivos no barramento. Qualquer dispositivo configurado para receber os dados é chamado assinante. Esse mecanismo é tipicamente usado para transferência cíclica e regular de dados de controle entre dispositivos no barramento.

Nas porções da largura de banda não ocupadas pela transmissão de mensagens CDs, o LAS envia um *pass token* (PT) para cada nó incluído numa lista específica. Cada *token* é associado com um intervalo máximo de duração, durante o qual o nó pode transmitir. Ao expirar este intervalo ou quando a transmissão é encerrada, o *token* retorna ao LAS através do quadro RT (*return token*).

A lista contendo os dispositivos que receberão o PT é chamada "*live list*". Após adicionar ou remover um dispositivo da lista, o LAS envia as mudanças a todos os dispositivos. Isso permite que cada dispositivo do tipo mestre de enlace mantenha uma cópia atual da lista, caso seja preciso assumir o papel do LAS.

O LAS envia periodicamente uma mensagem TD (*time distribution*) para que todos os dispositivos tenham exatamente o mesmo tempo no enlace de dados. Tanto as comunicações agendadas na rede quanto as execuções programadas dos blocos de função na camada de usuário são baseadas na temporização originada dessas mensagens.

Na camada de enlace, os dispositivos são identificados com um endereço de enlace, que consiste de três campos: *Link*, *Node* e *Selector* [18]. Estes campos estão expostos na Figura 11. O campo *Link* consiste de 16 *bits* e identifica um dispositivo de interconexão do tipo *link*. Quando a comunicação ocorre dentro de um mesmo segmento este campo é geralmente omitido. Este campo é necessário quando uma mensagem é repassada para outros segmentos através de pontes (*bridges*). O campo *Node*, com 8 *bits*, carrega o endereço do nó. Um dispositivo tem um endereço de nó na faixa entre 0x10 e 0xFF, permitindo endereçar até 240 dispositivos. Esta faixa de endereços é subdividida

em faixa LM, faixa básica, faixa padrão e faixa temporária. Geralmente, os dispositivos estão nas faixas LM ou básica, de acordo com a classe do dispositivo. Quando um dispositivo perde seu endereço de nó, ele se comunica usando um endereço da faixa padrão. Dispositivos temporários, como equipamentos portáteis, utilizam um endereço da faixa temporária. O LAS possui o endereço 0x04 [18]. O campo *Selector* fornece um endereço, de 8 *bits*, interno ao dispositivo para identificar o tipo de mensagem na aplicação.
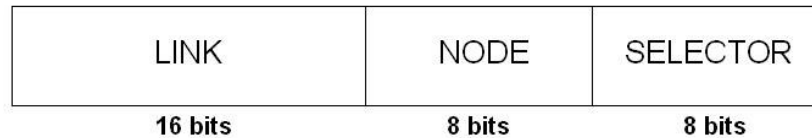
Figura 11 - Campos de endereçamento no FOUNDATION Fieldbus

A camada de aplicação H1 inclui duas subcamadas: subcamada de acesso ao barramento, e subcamada de especificação de mensagens. A subcamada de acesso ao barramento (FAS – *fieldbus acess sublayer*) usa as características da camada de enlace para prover serviços a subcamada de especificação de mensagens (FMS – *fieldbus message specification*).

Cada tipo de serviço FAS é descrito por uma relação de comunicação virtual, a VCR (*virtual communication relationship*). A VCR define o tipo de informações (mensagens) trocadas entre duas aplicações.

Os tipos de VCR definidos pelo FOUNDATION Fieldbus são:

- Cliente-servidor: usado para comunicação um para um, com fila e não-agendada, entre dois dispositivos no barramento. Quando um dispositivo recebe um PT do LAS, deve enviar uma requisição a outro dispositivo na rede. O dispositivo que faz a requisição é chamado de cliente e o que recebe a requisição é chamado de servidor. O servidor responde à requisição assim que receber o PT do LAS. O VCR cliente-servidor é usado para requisições iniciadas pelo operador como mudança de *set-point*, acesso e modificação de parâmetros de sintonia, manipulação de alarmes, e *upload* e *download* de dispositivos;
- Distribuição de boletins: usado para comunicação um para muitos, enfileirada e não-agendada. Quando um dispositivo, que possui um evento ou um boletim para enviar, recebe o PT do LAS, ele envia a mensagem a um grupo de endereços definido pela VCR. Normalmente utilizada para notificação de alarmes;
- Editor-assinante (*publisher-subscriber*): usado para comunicação um para muitos com *buffer*. Quando um dispositivo recebe um CD (*compel data*) deve publicar, em *broadcast*, sua mensagem a todos os dispositivos no barramento. Os dispositivos que desejam receber a mensagem publicada são chamados de assinantes.

Os serviços da subcamada FMS permitem que aplicações de usuários troquem mensagens

através do barramento. A FMS descreve os serviços de comunicação, formatos de mensagens e comportamento de protocolo, necessários à construção de mensagens da aplicação. Os dados são descritos por uma descrição de objeto. Estes são reunidos em um dicionário de objetos. A descrição de objeto é identificada pelo seu índice no dicionário.

Um VFD (*virtual field device*) é usado para visualizar remotamente os dados de um dispositivo local, descritos no dicionário de objetos. Um típico dispositivo tem pelo menos dois VFDs: VFD de gerenciamento de rede e sistema, e VFD de aplicação de usuário. O VFD de gerenciamento provê acesso à base de informações de gerenciamento da rede (NMIB) e à base de informações de gerenciamento do sistema (SMIB).

O VFD de aplicação é usado para tornar as funções do dispositivo visíveis ao sistema de comunicação do *fieldbus* (a função de um dispositivo é definida pela seleção e interconexão dos blocos). Em geral, todos os serviços FMS usam o VCR tipo cliente-servidor, exceto alguns casos especiais [8].

Dentro das especificações do FOUNDATION Fieldbus H1, o gerenciamento do sistema lida com aspectos importantes tais como:

- <u>Agendamento de bloco de função</u>. Blocos de função devem ser executados em intervalos precisamente definidos e na seqüência apropriada para uma correta operação do sistema de controle. Um macro-ciclo é uma única iteração de um agendamento no dispositivo. Dependendo do tipo de dispositivo, é possível ter um macro-ciclo de LAS e um macro-ciclo de dispositivo. No primeiro, o gerenciamento sincroniza a execução dos blocos de função ao longo de todo o enlace *fieldbus*. Já no segundo caso, o gerenciamento sincroniza a execução de blocos de função dentro de cada dispositivo;
- <u>Distribuição do relógio de aplicação</u>. O gerenciamento possui um divulgador que periodicamente envia uma mensagem de sincronização para todos os dispositivos;
- <u>Designação de endereço de dispositivo</u>. Cada dispositivo deve ter um endereço de rede único. A designação é feita da seguinte maneira: um dispositivo não configurado se junta à rede em um dos quatro endereços temporários especiais, uma ferramenta de configuração atribui uma etiqueta de dispositivo físico ao novo dispositivo, em seguida é selecionado um endereço permanente não utilizado para ser designado ao dispositivo. A seqüência é repetida para todos os dispositivos que entrem na rede;
- <u>Serviço de busca de etiquetas</u>. O gerenciamento de sistema suporta um serviço para encontrar dispositivos ou variáveis através de uma busca de etiquetas. A mensagem de busca é difundida a todos os dispositivos, após receber a mensagem cada dispositivo procura em seus VFDs pela etiqueta solicitada e, caso seja encontrada, retorna as informações de caminho (incluindo endereço de rede, número do VFD, índice de VCR e índice do dicionário de objetos).

Na Figura 12 é mostrada a estrutura de quadros na pilha de protocolos do FOUNDATION Fieldbus.
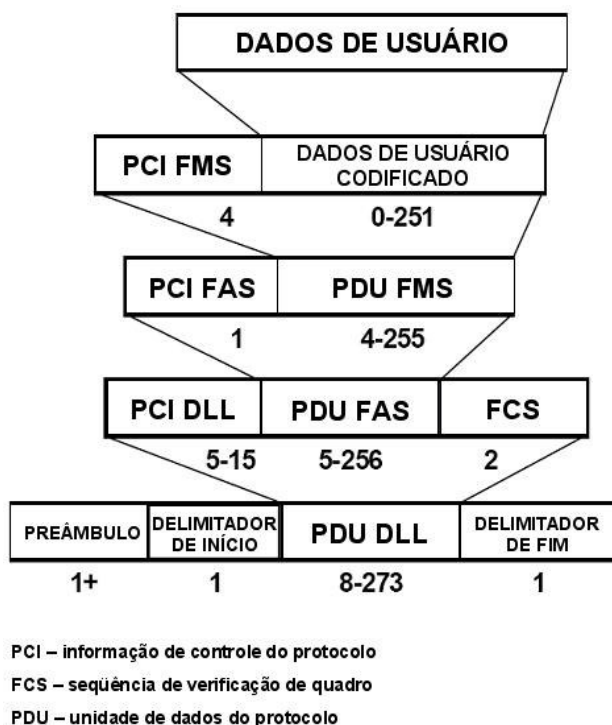
Figura 12 - Estrutura de quadros do FOUNDATION Fieldbus

2.2.2. FOUNDATION Fieldbus HSE

O FOUNDATION Fieldbus HSE define uma camada de aplicação e funções de gerenciamento associadas, projetada para operar sobre uma pilha TCP/UDP/IP padrão, sobre Ethernet de par trançado ou fibra ótica. Principalmente prevista para aplicações de manufatura discretas [8], pode ser usado para interconectar segmentos H1, assim como protocolos externos através de *gateways* TCP/IP com o objetivo de construir redes de planta completas.

A Fieldbus Foundation inicialmente planejou adotar o padrão IEC/ISA de alta velocidade, mas recentemente decidiu usar o HSE (*high-speed ethernet*) devido principalmente à grande disponibilidade de componentes e à existência de redes nas plantas (pelo menos em nível de *backbone*) [7]. A principal característica do FOUNDATION Fieldbus – HSE é o uso da arquitetura de Internet (TCP/UDP/IP e IEEE 802.3u) para o controle discreto em alta velocidade e, de forma mais geral, para interconectar diversos segmentos H1 com o objetivo de alcançar uma rede *fieldbus* em toda a planta.

O HSE opera à 100 Mbps e pode ser equipado por linhas elétricas (par trançado) ou cabos de fibra ótica. A Ethernet utiliza o protocolo CSMA de acesso ao meio [17]. No protocolo CSMA (*Carrier Sense Multiple Acess*), quando uma estação deseja transmitir, ela primeiro escuta o canal de comunicação para verificar se outra estação está transmitindo naquele momento. A transmissão

só é efetuada se o canal estiver ocioso.

Se a carga do barramento deve ser reduzida devido à quantidade de dispositivos conectados, ou se várias sub-redes HSE serão combinadas para criar uma grande rede, *switches* Ethernet devem ser usados. Um *switch* lê o endereço de destino do pacote de dados a ser repassado e então direciona o pacote à sub-rede correspondente [17].

Existem quatro categorias básicas de dispositivos HSE: dispositivo de enlace, dispositivo Ethernet, dispositivo *host* e dispositivo *gateway* [8]. Um dispositivo de enlace conecta redes H1 às redes HSE. Um dispositivo Ethernet pode executar blocos de função e pode ter I/Os convencionais. Um dispositivo *gateway* faz a interface com outros protocolos de rede como Modbus, DeviceNet ou PROFIBUS. Um dispositivo *host* é um dispositivo não-HSE capaz de comunicação com dispositivos HSE. Exemplos incluem terminais de configuração, estações de operadores e servidores OPC.

Componentes padrões da pilha HSE são: DHCP (*Distributed Host Configuration Protocol*) que designa os endereços; SNTP (*Simple Network Time Protocol*) e SNMP (*Simple Network Management Protocol*), que confiam no TCP e UDP sobre IP; e o IEEE 802.3 MAC e camada física. Isto resultou em um número de nós (endereços IP) praticamente ilimitado [8], sobre redes em topologia estrela feitas de quantos *links* necessários. O comprimento pode chegar até 100 metros em par trançado e dois quilômetros em fibra ótica.

As mensagens enviadas na Ethernet são limitadas por uma série de campos de dados chamados quadros. A combinação de uma mensagem e um quadro é chamada pacote Ethernet. Tipicamente, um pacote codificado de acordo com TCP/IP será inserido no campo de mensagem do pacote Ethernet. FOUNDATION Fieldbus usa uma estrutura de dados similar, onde as mensagens são limitadas pelo endereçamento e outros itens de dados. O que corresponde a um pacote no Ethernet é chamado PDU (*protocol data unit*) no FOUNDATION Fieldbus.

A solução desenvolvida pelo FOUNDATION Fieldbus para a comunicação entre dois dispositivos H1 com um segmento HSE entre eles é mais complexa, porém mais eficiente que o tunelamento usado em redes TCP/IP usuais [8]. O PDU HSE é inserido no campo de dados de um campo de mensagens TCP/IP. Entretanto, o endereço *fieldbus* é codificado como um único endereço TCP/IP, de forma que o endereço do PDU é usado para preencher o campo de endereço do pacote TCP/IP. O pacote TCP/IP é então inserido no campo de mensagem do pacote Ethernet. Devido ao esquema de codificação HSE, redes contendo vários dispositivos de enlace podem localizar e transferir mensagens ao destino correto mais rapidamente. Talvez ainda mais importante: cada dispositivo H1 (e consequentemente cada dispositivo HSE) tem um endereço TCP/IP único e pode ser diretamente acessado através de redes Internet e TI.

As novas tecnologias são baseadas no agente FDA (*field device acess*). O agente FDA permite que serviços FMS e de gerenciamento usados em dispositivos H1 sejam transportados na

Ethernet usando TCP e UDP. Permitindo dispositivos HSE se comunicarem com dispositivos H1 conectados por um dispositivo de enlace. O agente FDA é também usado pelos blocos de função locais em dispositivos HSE. Assim, o agente FDA habilita aplicações remotas a acessar dispositivos H1 e HSE através de uma interface comum.

Os seguintes aspectos de gerenciamento são fornecidos pela camada de gerenciamento de sistema HSE: cada dispositivo tem uma identidade única e permanente, e um nome de sistema específico configurado; os dispositivos mantêm informações de controle de versões; dispositivos respondem a solicitações que desejam localizar objetos, incluindo o próprio dispositivo; o tempo é distribuído a todos os dispositivos na rede; os agendamentos de blocos de função são usados para executar blocos de função; dispositivos são adicionados ou removidos da rede sem afetar os demais.

As operações de redundância não são visíveis às aplicações HSE. Cada dispositivo transmite periodicamente na Ethernet uma mensagem de diagnóstico, representando sua visão da rede. Cada dispositivo usa essas mensagens para manter uma tabela de estado da rede, usada para detecção de falhas e para selecionar a porta de transmissão (já que cada dispositivo escolhe a melhor rota para cada mensagem que deseja enviar) [8]. Não há um gerenciador central de redundância.

2.3. Estudo Comparativo entre PROFIBUS DP e FOUNDATION Fieldbus H1

Uma comparação entre as redes PROFIBUS DP e FOUNDATION Fieldbus H1 é exibida na Tabela 3. Ambas possuem características que as habilitam para aplicação em automação de processos, inclusive em áreas classificadas.

Tabela 3 - Comparativo entre PROFIBUS DP e FOUNDATION Fieldbus H1.

	PROFIBUS DP	**FOUNDATION Fieldbus H1**
Taxa de transferência	9,6 kbps à 12 Mbps	31,25kbps
Nº máximo de estações por segmento	32 estações	32 estações
Capacidade de endereçamento na rede	126 endereços	240 endereços
Comprimento de carga útil	246 bytes	251 bytes
Tipos de dispositivos	Mestre (DPM1, DPM2) ou escravo	Mestre de enlace ou básico
Quantidade de mestres na rede	Multimestre	Multimestre
Mecanismo de acesso ao meio	• Cíclico (dados): passagem de token entre mestres + mestre/escravo • Acíclico (alarmes e parâmetros): paralelo ao cíclico com baixa prioridade	• Comunicação agendada: editor-assinante • Com. não-agendada: cliente-servidor ou distribuição de relatórios

3. Tecnologia sem fio em plantas industriais

Vários são os benefícios agregados à adoção de transmissão sem fio. O principal deles é a ausência de cabos para prover a comunicação entre as estações, diminuindo custos com instalação e manutenção, além de eliminar possíveis pontos de falha difíceis de serem localizados. Outros fatores favoráveis são: flexibilidade na montagem e modificação da estrutura, e mobilidade dos instrumentos.

Em plantas industriais, a tecnologia sem fio pode ser usada de várias maneiras interessantes [10]:

- Disponibilização de serviços de comunicação para aplicações de controle distribuído, envolvendo subsistemas móveis como veículos de transporte autônomos, robôs, etc.;
- Implementação de sistemas de controle distribuído em áreas explosivas ou na presença de agentes químicos agressivos;
- Fácil reconfiguração freqüente da planta, já que poucos cabos precisam ser remontados;
- Sistemas móveis de diagnósticos da planta e estações sem fio para programação e configuração.

O emprego de redes de sensores sem fio em plantas industriais, especialmente na indústria de processos, tem se tornado uma solução interessante.

A adoção de tecnologia sem fio, contudo, acarreta alguns problemas. O primeiro é a disputa entre a alta confiabilidade e requisitos de tempo exigidos pelas aplicações industriais, e os problemas inerentes aos canais sem fio. O segundo grande problema é o desejo de integrar estações cabeadas e estações sem fio numa única rede, o que exige o desenvolvimento de protocolos interoperáveis. Além disso, o uso da tecnologia sem fio traz problemas não vislumbrados no desenvolvimento dos sistemas cabeados: segurança e interferência [10].

A transmissão de formas de onda está sujeita a fenômenos como atenuação, reflexão, difração, dispersão, interferência de canal adjacente e de co-canal, ruído térmico ou produzido por outras fontes, e imperfeições nos circuitos de transmissão e recepção [10].

Para protocolos de acesso ao canal baseados na detecção de portadora (CSMA) ocorrem problemas de estação oculta e estação exposta [2].

Diferentes técnicas de transmissão têm sido desenvolvidas para combater as imperfeições do canal sem fio e para aumentar a confiabilidade da transmissão de dados. Muitos tipos de WLANs (*Wireless Local Area Networks*) usam técnicas de espalhamento espectral, onde um sinal de informação em banda estreita é espalhado em um sinal de banda larga no transmissor e "reagrupado" no receptor. Ao usar um sinal banda larga, os efeitos de ruído ou interferência de

banda estreita são reduzidos. As duas principais técnicas de espalhamento espectral são: espalhamento espectral de seqüência direta (DSSS – *direct sequence spread spectrum*) e espalhamento espectral por saltos na freqüência (FHSS – *frequency-hopping spread spectrum*).

Com relação à segurança, a instrumentação sem fio se protege lançando mão de duas principais técnicas [36]:

- Mantendo os sinais confinados ao usar cuidadosamente as potências dos transmissores. Isto minimiza o potencial dos dados se espalharem além dos perímetros da planta onde *hackers* possam bisbilhotar ou atacar;
- Combinando técnicas de criptografia e autenticação. Os dados enviados não são apenas cifrados, mas os instrumentos também têm que se identificar para participar da rede.

Diversos são os padrões para uso de comunicação sem fio entre dispositivos. Os principais são: Wi-Fi, Bluetooth e ZigBee. O primeiro é descrito na norma IEEE 802.11, o segundo na norma IEEE 802.15.1 e o último na IEEE 802.15.4. A Tabela 4 contém as principais características destes três padrões.

Tabela 4 - Características dos principais padrões de rede sem fio.

	Wi-Fi	**Bluetooth**	**ZigBee**
Taxa de transferência	11 a 54 Mbps	1 Mbps	20 a 250 kbps
Número de nós	Mais de 100	Até 8	Até 65535
Alcance	100m	100m	100m
Técnica de transmissão	DSSS e OFDM	FHSS	DSSS
Corrente de consumo (típica)	350 mA	65 a 170 mA	30 mA
Vida útil da bateria	1 a 3 horas	1 a 7 dias	Até 2 anos

Apesar de possuir uma taxa de transferência inferior a dos outros dois padrões, o ZigBee é vantajoso com relação ao número de nós suportados numa rede. Outra vantagem é o baixo consumo de energia que facilita o uso de baterias como fonte de alimentação dos dispositivos. Por essas razões o ZigBee foi selecionado para ser o padrão responsável pela rede de comunicação sem fio.

3.1. Redes de Sensores Sem Fio

As redes de sensores sem fio (RSSFs) são constituídas por um grande número de nós que são distribuídos em uma área onde determinada aplicação será executada. As RSSFs têm como objetivo monitorar e, eventualmente, controlar um ambiente. Informações são coletadas e roteadas em direção ao nó *sink*. Um nó *sink* é um *gateway* entre as redes de sensores e uma rede externa, sendo de vital importância para a execução das aplicações [29].

Os principais componentes de um nó sensor são transceptor para comunicação sem fio, fonte de energia, unidade de sensoriamento, memória e processador. Existem casos em que uma

RSSF também pode ser composta de dispositivos chamados atuadores que permitem ao sistema controlar parâmetros do ambiente monitorado [27].

Sem perda de generalidades, no restante deste documento, um conjunto de dispositivos contendo sensores e atuadores que utilize um meio de transmissão sem fio também será denominado de rede de sensores sem fio.

Em geral, as redes em ambientes industriais que utilizam protocolos sem fio necessitam de uma série de fatores em seu desenvolvimento: alcance, taxa de transmissão, latência, consumo de energia, número de dispositivos, flexibilidade, confiabilidade.

Fatores, como alcance, taxa de transmissão e latência, não necessitam de valores altos. Dependem muito do tipo de aplicação. O consumo de energia deve ser o mais eficiente possível, com um longo tempo de vida das baterias. O número de dispositivos deve ser tal que satisfaça as necessidades da aplicação.

Alguns nós sensores em uma RSSF podem falhar devido à falta de energia, danos físicos ou interferência do ambiente. Essa falha não deve afetar a execução da rede [28]. A tolerância à falhas é a habilidade de sustentar as funcionalidades da rede de sensores sem interrupções devido à falhas de nós.

A maneira mais óbvia de conservar energia é desligar o transceptor quando este não for requerido. Embora este método pareça fornecer ganhos de energia significativos, um ponto importante que não deve ser esquecido é que os nós se comunicam usando pequenos pacotes de dados. O modo de conservação de energia é eficiente somente se o tempo gasto neste modo for maior que certo limiar [28]. Isso devido à energia gasta para religar o transceptor. Como os nós sensores são operados por baterias, os protocolos devem ser eficientes na utilização de energia para maximizar a vida útil do sistema.

Esquemas de modulação, estratégias para superar os efeitos da propagação de sinal e projeto de hardware de baixo consumo são requisitos do projeto da camada física. Esquemas de controle de erro, modos de operação para economizar energia e cuidados com a mobilidade são os desafios da camada de enlace e dos protocolos de controle de acesso ao meio. Tratar das mudanças de topologia, endereçamentos, escalabilidade e interface com outras redes são requisitos esperados para a camada de rede [27].

A aplicação influenciará diretamente nas funções exercidas pelos nós da rede, assim como na arquitetura desses nós (processador, memória, dispositivos sensores, fonte de energia, transceptor), na quantidade de nós que compõem a rede, na distribuição inicialmente planejada para a rede, no tipo de deposição dos nós no ambiente, na escolha dos protocolos da pilha de comunicação, no tipo de dados que será tratado, no tipo de serviço que será fornecido pela rede e consequentemente no tempo de vida dessa rede.

Capacidade de monitoramento remoto, robustez, e a flexibilidade de configuração e

manutenção, vinculados com as características relacionadas anteriormente fazem da RSSF uma potencial ferramenta para as aplicações da indústria de petróleo e gás natural. A ausência de cabeamento físico presente nas redes de sensores em fio torna esta tecnologia uma grande candidata para inserção em refinarias e plataformas de petróleo [29], onde os espaços físicos das aplicações devem ser otimizados usando as técnicas mais flexíveis.

3.2. ZigBee

ZigBee é um protocolo de rede sem fio, desenvolvido pela ZigBee Alliance, direcionado para aplicações de automação e controle remoto, tentando prover baixo custo e baixo consumo para conectar equipamentos que necessitam de bateria duradoura mas não requerem altas taxas de transferência de dados [20].

ZigBee Alliance é constituída por mais de 200 empresas, oriundas de mais de 20 países distintos, na qual se integram também especialistas da área de telecomunicações e semicondutores, incluindo membros do IEEE.

A arquitetura ZigBee é baseada no modelo OSI mas define apenas as camadas relevantes para alcançar as funcionalidades desejadas. Cada camada executa um conjunto de serviços para a camada superior: uma entidade de dados provê um serviço de transmissão de dados e uma entidade de gerenciamento provê todos os outros serviços [25]. A especificação ZigBee define as camadas de rede e aplicação, e o serviço de segurança entre elas. A definição das camadas física e de acesso ao meio é de responsabilidade da norma IEEE 802.15.4 [22]. As camadas ZigBee podem ser vistas na Figura 13 .
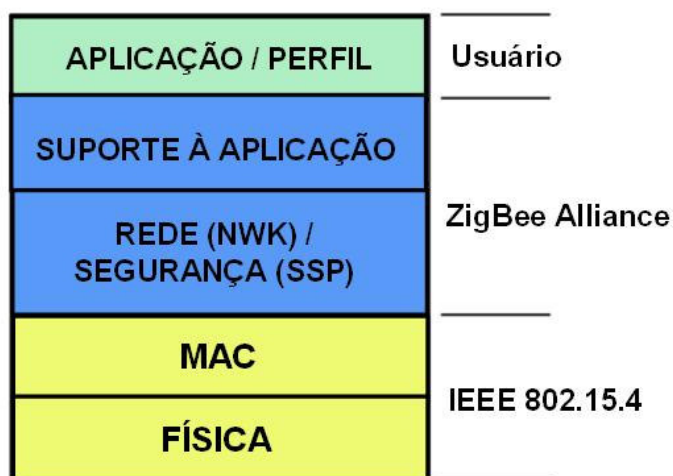
Figura 13 - As camadas do ZigBee

A camada física provê a comunicação no meio físico. A camada MAC fornece serviços que permite comunicação ponto a ponto (um salto) confiável entre dispositivos. A camada de rede ZigBee provê roteamento e funções de múltiplos saltos necessárias para criar diferentes topologias.

A camada de aplicação inclui uma subcamada APS de suporte à aplicação, o objeto de dispositivo ZigBee (ZDO) e as aplicações definidas pelos fabricantes. O ZDO é responsável por todo o gerenciamento do dispositivo [25].

ZigBee é mais apropriado para aplicações que envolvam dispositivos remotos alimentados por baterias, nomeadamente sensores e atuadores, já que permite baixos consumos, taxas aceitáveis e possui uma pilha protocolar mais simples que possibilita a sua implementação em sistemas com recursos limitados.

3.2.1. Arquitetura

Com uma vasta área de aplicação, desde o controle industrial até automação doméstica, o protocolo ZigBee possui as seguintes características:

- Reduzido consumo de potência;
- Pilha de protocolos simplificada;
- Possibilidade de suportar elevada densidade de nós por rede (máximo de 65535 por cada coordenador, contra 7 do Bluetooth e 30 do Wi-Fi);
- Diferentes topologias: estrela, em malha e árvore;
- Tempo de associação à rede menor que outros protocolos;
- Apenas dois estados de operação: *active* e *sleep*;
- Dois modos de operação da rede: com sinalização e sem sinalização;
- Os dispositivos podem ser de três tipos: coordenador, *router* e *end device*;
- Elevada segurança, com recurso a criptografia de 128 bits.

Um dispositivo ZigBee pode ser um FFD (*full-function device*) ou um RFD (*reduced-function device*). Uma rede deve possuir pelo menos um FFD, operando como coordenador da PAN (*personal area network*). Um RFD é direcionado para aplicações extremamente simples que não necessitam enviar grandes quantidades de dados. Um dispositivo FFD pode conversar com RFDs ou FFDs, enquanto que um RFD pode conversar apenas com um FFD. Comunicação direta entre RFDs não é possível, é preciso que os pacotes passem por um FFD [9].

Dispositivos RFDs podem buscar redes disponíveis, transferir dados de sua aplicação quando necessário, determinar se há dados pendentes, requisitar dados do coordenador, e dormir por longos períodos para reduzir o consumo de bateria. Dispositivos FFDs descobrem outros FFDs e RFDs para estabelecer comunicação, e podem ser alimentados pela rede elétrica.

Os tipos de dispositivos lógicos são coordenador, *router* e *end device*. O primeiro é responsável pela criação e manutenção da rede ZigBee, armazenando informação de gestão interna relevante para o seu funcionamento, atribuir endereços aos dispositivos, e podendo também funcionar como ponte (*bridge*) entre diferentes redes ZigBee. Deve ser um dispositivo do tipo FFD. O *router*, além de ser um nó normal tem como funcionalidade extra poder funcionar como um

roteador intermediário, permitindo a comunicação entre nós sem a intervenção do coordenador. Deve ser um dispositivo do tipo FFD. O terceiro tipo, *end device*, apenas tem a possibilidade de comunicar com a rede, não tendo nenhuma função de gestão, e não executa qualquer das outras funções ZigBee. Pode ser um dispositivo FFD ou RFD.

ZigBee suporta as topologias estrela, em malha e em árvore, ilustradas na Figura 14.
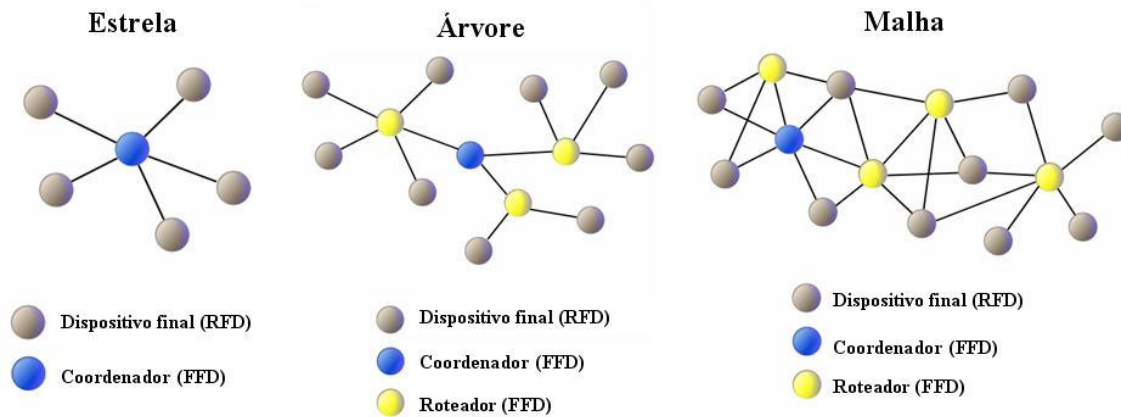
Figura 14 - Topologias ZigBee: estrela, árvore e malha

Numa topologia estrela, uma rede ZigBee requer um dispositivo FFD atuando como coordenador da rede e os demais dispositivos podem ser RFDs para reduzir o custo. Após um dispositivo FFD ser acionado pela primeira vez, sua própria rede é estabelecida e este se torna o coordenador da rede. Cada rede escolhe um identificador da PAN único no raio de alcance da rede. Assim, cada rede opera independentemente. Redes em estrela são comuns e fornecem longa vida de operação às baterias.

Na topologia em malha também há um coordenador da PAN, mas o coordenador e os *routers* são livres para comunicar com outro dispositivo FFD. Isto permite a expansão física da rede (maior alcance). O coordenador registra toda a entrada e saída dos dispositivos, mas não assume um papel centralizador do fluxo de informações como ocorre na topologia estrela. Os *routers* na topologia em malha não devem emitir pacotes de sinalização. Redes em malha permitem alto nível de confiabilidade e escalabilidade ao prover mais de um caminho dentro da rede. Aplicações como monitoramento e controle industrial, e redes de sensores, são beneficiadas com essa topologia.

Uma rede em árvore é um caso especial de redes em malha, em que a maioria dos dispositivos são FFDs, e os RFDs ficam localizados nas extremidades da árvore. Qualquer FFD pode atuar como coordenador, provendo serviços de sincronização, mas apenas um será o coordenador da PAN. Na topologia em árvore efetua-se a distribuição de dados e mensagens de controle numa estrutura hierárquica, onde o coordenador assume o papel de nó "nuclear" da rede. Redes em árvore utilizam uma topologia híbrida estrela/malha que combina os benefícios de ambas para alta confiabilidade e suporte a nós alimentados por baterias. Pode ser empregada a comunicação com sinalizadores.

Redes ZigBee consistem de diferentes tipos de tráfego, cada um com suas características únicas:

- Dados periódicos: dados são tipicamente manipulados usando um sistema com sinalizador, onde o dispositivo acorda em certo tempo e verifica o pacote de sinalização, troca dados, e volta a dormir (retorna ao modo *sleep*). Comum em aplicações do tipo sensores.
- Dados intermitentes: dados são manipulados em um sistema sem sinalização ou desconectado. No modo de operação desconectado, o dispositivo "participa" da rede quando é preciso comunicar, salvando energia. Usualmente aplicado em aplicações definidas ou com estímulo externo, como interruptores de luz.
- Dados repetitivos com baixa latência: usa a capacidade de reserva de *time slots*. Método de QoS (*Quality of Service* – Qualidade de Serviço) que atribui ao dispositivo um período de tempo específico, definido pelo coordenador, no super-quadro para realizar o que desejar sem disputa ou latência. Usados em aplicações como sistemas de segurança.

Em todas as aplicações, por menor que seja o pacote dos dispositivos ZigBee, resulta em um *throughput* efetivo alto comparado com outros padrões [24].

Um novo nó pode ser reconhecido e associado à rede ZigBee em aproximadamente 30 ms. Acordar um nó dormente, ou seja, fazer com que o nó operando no estado *sleep* entre no estado *active*, leva cerca de 15 ms, assim como acessar um canal e transmitir dados [24]. As aplicações ZigBee se beneficiam da habilidade de rapidamente anexar informações, desanexar e ir dormir, o que resulta em baixo consumo de energia e duração extendida de bateria.

Em termos de endereçamento de dispositivos, endereços longos são implementados na camada MAC pelo fabricante e têm 64 *bits* de comprimento. Endereços curtos, por outro lado, são atribuídos dinamicamente e têm 16 *bits* de comprimento. Endereçamento curto é usado pela simplicidade e para reduzir requisitos de armazenamento na plataforma de hardware.

Cada rede ZigBee precisa de um coordenador que pode manipular até 255 dispositivos no caso de endereçamento com 16 bits, e no máximo 65535 nós no caso de 64 bits.

A cada nó é dado um endereço quando este se junta à rede ZigBee. Um nó contém uma ou mais descrições de dispositivos e possui um único rádio IEEE 802.15.4. As partes individuais dos nós são subunidades contendo uma descrição de dispositivo em cada subunidade.

ZigBee provê um nível de sub-endereçamento, usado em conjunto com o mecanismo do IEEE 802.15.4. Um número de *endpoint* pode ser usado para identificar as subunidades individualmente. Cada subunidade é identificada pelo seu *endpoint* específico na faixa de 1 a 240.

Um comando é enviado para um objeto de aplicação no endereço de destino (endereço de rádio mais *endpoint*). Um endereço IEEE 802.15.4 completo ocupa 10 octetos (identificador da PAN mais endereço IEEE de 64 bits) e mais um octeto é necessário para o *endpoint*.

A camada SSP (*security service provider*) fornece serviços de segurança, estabelecendo e trocando chaves de segurança, e usando estas chaves para fixar as comunicações. A arquitetura inclui mecanismos de segurança em três camadas da pilha de protocolos. As camadas MAC, de rede e de aplicação são responsáveis pelo transporte seguro de seus respectivos quadros. A regra geral é que a camada responsável para gerar um quadro de dados é responsável por codificá-lo quando envia, e autenticá-lo quando recebe [25]. Além disso, a subcamada APS dispõe serviços para o estabelecimento e manutenção de relações seguras. O ZDO gerencia as políticas de segurança e a configuração de segurança de um dispositivo.

3.2.2. Camada física e camada MAC

O padrão IEEE 802.15.4 opera em três possíveis freqüências: 2,4 GHz (global), 915 MHz (América do Norte) e 868 MHz (Europa), pertencentes à faixa ISM (*Industrial, Scientific and Medical*), que não requer licença para funcionamento. No Brasil, em princípio, a freqüência usada será a de 2,4 GHz [21]. As taxas de transmissão são: 250 kbps em 2,4 GHz, 40 kbps em 915 MHz e 20 kbps em 868 MHz. A freqüência de transmissão mais elevada provê uma maior taxa de dados e menor latência. As freqüências mais baixas promovem maior alcance e melhor sensibilidade. ZigBee utiliza espalhamento espectral por seqüência direta (DSSS) com modulação O-QPSK (*offset-quadrature phase shift keying*) na banda 2,4 GHz. Nas bandas de 915 e 868 MHz também é usado DSSS, mas com modulação BPSK (*binary phase shift keying*). A norma IEEE 802.15.4 usa a tecnologia DSSS porque a alternativa FHSS (*frequency hop spread spectrum*) tende a gastar mais energia ao pular de freqüência para manter seu sincronismo [21]. Há um único canal presente na faixa de 868 MHz, 10 canais na faixa de 915 MHz, e 16 canais na faixa de freqüências de 2,4 GHz. Diversos canais presentes na faixa de freqüências possibilitam a realocação dentro do espectro. As sensibilidades dos receptores são: -85 dBm em 2,4 GHz e -92 dBm em 868/915 MHz [20]. O padrão oferece um alcance de transmissão até 100 m, dependendo da potência dos equipamentos e de características ambientais (obstáculos físicos, interferência eletromagnética, etc.).

Características da camada física são ativação e desativação do rádio transceptor, detecção de energia, indicação de qualidade do link, seleção de canal, e transmissão e recepção de pacotes através do meio físico. A detecção de energia é uma estimativa da potência do sinal recebido dentro de um canal. O resultado da medição deve ser reportado em um inteiro de oito bits. O valor mínimo da medida (zero) deve indicar uma potência de 10 dB abaixo da sensibilidade especificada no receptor [20]. A indicação de qualidade do link é uma caracterização da qualidade de um pacote recebido. O uso desse indicador fica a cargo das camadas de rede e de aplicação. O resultado do indicador é um inteiro de 8 *bits* [20].

Existem quatro pacotes de estrutura de dados, cada uma designada de unidade de protocolo de dados da camada física (PPDU) no padrão de transações de dados: um quadro de sinalização, um

quadro de dados, um quadro de reconhecimento e um quadro de comando MAC. Todos os quadros são estruturados de forma similar, com a principal diferença em seu objetivo ou carga. Cada pacote PPDU (*physical protocol data unit*) consiste dos seguintes componentes básicos: SHR, que permite sincronização; PHR, que contém informação sobre o tamanho do quadro; e uma carga (*payload*) de tamanho variável, contendo o quadro da subcamada MAC. Esta estrutura é vista na Figura 15. Campos do pacote da camada física: preâmbulo (32 *bits*), responsável pela sincronização de símbolo; delimitador do início de pacote (oito *bits*), que faz a sincronização do quadro; cabeçalho PHY (oito *bits*), que especifica o comprimento do PSDU; PSDU (até 127 *bytes*), que é o campo de dados.

Bytes: 4	1	1		variável
Preâmbulo	SFD	Tamanho do quadro (7 bits)	Reservado (1 bit)	PSDU
SHR		PHR		Carga PHY

Figura 15 - Estrutura do quadro na camada física do ZigBee

O MPDU (MAC *protocol data unit*) é construído com um cabeçalho MAC (MHR), um rodapé MAC (MFR) e uma unidade de serviços de dados MAC (MSDU), como apresentado na Figura 16. A única exceção ocorre com o MPDU do quadro de reconhecimento, que não contém um MSDU. O MSDU é um campo de dados (uma carga) que compõe um determinado quadro contendo informações pertinentes aos serviços MAC suportados pelo quadro.

Bytes: 2	1	0/2	0/2/8	0/2	0/2/8	variável	2
Controle de quadro	Número de seqüência	End. PAN destino	End. destino	End. PAN fonte	End. fonte	Carga do quadro	FCS
		Campos de endereçamento					
MHR						Carga MAC	MFR

Figura 16 - Estrutura do quadro MAC no ZigBee

O MAC do 802.15.4 abrange toda a camada de enlace, não sendo uma subcamada. A camada de enlace padrão normalmente consiste em duas subcamadas: a subcamada MAC e a subcamada LLC. Entretanto, o padrão 802.15.4 não usa uma subcamada LLC separada, ao invés disso incorpora suas funcionalidades numa subcamada MAC melhorada. Tal abordagem provê simplicidade na operação e implementação [23]. À camada MAC cabe o papel de controlar o acesso aos canais RF. Além disso, especifica os tipos de dispositivos permitidos na rede, a estrutura de quadros, sincronização e transmissão de quadros de sinalização.

A princípio, o acesso ao meio pode ser feito de três formas: CSMA/CA (*Carrier Sense*

Multiple Acess – Collision Avoidance) sem sinalizadores, CSMA/CA no período com disputa em um sistema com sinalizadores, ou com reserva de *time slots* no período sem disputa em sistemas com sinalizadores. Tanto o método de acesso ao canal com disputa quanto o método sem disputa suportam um tamanho máximo de pacote que inclua uma carga variável de até 102 bytes [24].

No modo com sinalização, os nós *routers* transmitem periodicamente um sinalizador (*beacon*) para confirmar sua presença a outros nós na rede. O intervalo entre *beacons* varia de 15,36 ms a 251,65 s, para uma taxa de 250 kbps. Como os nós só precisam estar ativos no momento da sinalização, permanecendo no estado *sleep* durante este intervalo, há uma redução de consumo energético. No entanto, é preciso levar em conta que intervalos longos entre *beacons* requerem uma sincronização de elevada precisão, o que aumenta a complexidade de implementação, aumentando o custo dos dispositivos.

Além disto, o padrão suporta um modo sem sinalização no qual a rede pode operar sem sinalizadores. Este modo permite que escravos, numa rede estrela mestre-escravo, por exemplo, permaneçam em repouso indefinidamente, somente entrando em contato com o mestre (que pode estar, talvez, conectado à rede elétrica e desta forma ser capaz de constante recepção) quando ocorrer um evento. Os escravos podem, portanto, ter uma duração quase ilimitada da bateria, determinada primordialmente pelo seu consumo de energia em repouso [21].

No modo *beacon*, normalmente os nós escravos dormentes despertam periodicamente para receber um sinal do *beacon* do nó de controle da rede. Este fato torna o consumo de energia no modo com sinalização maior do que no modo sem sinalização.

A transmissão do quadro de sinalização está disponível somente para FFD na rede. O quadro de sinalização é fornecido como um serviço originado na camada MAC do protocolo e possui interface com a camada física.

Redes IEEE 802.15.4 permitem o uso opcional de uma estrutura de super-quadro, cujo formato é definido pelo coordenador. O super-quadro é limitado pelos *beacons* e dividido em 16 *time slots*. O quadro *beacon* é enviado no primeiro *slot* de tempo. Os *beacons* são usados para sincronização, identificação da PAN e para descrever a estrutura dos super-quadros. O super-quadro pode ter uma porção ativa e uma porção inativa. Durante a porção inativa, o coordenador não interage com a PAN e fica no estado de baixa energia. O acesso ao meio ocorre através de um mecanismo CSMA/CA sem *time slots*. A porção ativa consiste em período de acesso disputado (CAP – *contention acess period*) e período livre de disputa (CFP – *contention free period*). Durante o CAP, um dispositivo que deseja transmitir tem que disputar com outros dispositivos usando um mecanismo CSMA-CA com *time slots*. Já o CFP contém *slots* de tempo garantido. O coordenador da PAN pode alocar até sete destes *time slots* garantidos [20]. O CFP vem sempre no final de super-quadro, após o CAP. Uma estrutura de super-quadro é mostrada na Figura 17.

Existem três tipos de transferência de dados: de coordenador para dispositivo, de

dispositivo para coordenador e entre dispositivos pares (iguais), não sendo ambos dispositivos do tipo RFD. O mecanismo de cada um destes tipos depende do suporte à transmissão de *beacons* pela rede. Quando um dispositivo deseja transferir dados em uma rede sem *beacon*, ele simplesmente transmite seu quadro usando CSMA-CA sem *slots* de tempo. Se a rede possuir sinalização, o dispositivo primeiro procura pelo *beacon* e em seguida sincroniza a estrutura de super-quadro. No tempo certo o quadro é transmitido ao coordenador. Quando um coordenador deseja transferir dados a um dispositivo em uma rede com sinalização, ele indica no *beacon* que uma mensagem de dados está pendente. Os dispositivos escutam o *beacon* periodicamente, e se há uma mensagem pendente direcionado a um dos dispositivos, este transmite um comando requisitando tais dados. O dispositivo transmite um quadro indicando o sucesso da recepção, e a mensagem é removida da lista de mensagens pendentes no *beacon*. Quando um coordenador deseja transferir dados a um dispositivo em uma rede sem sinalização, ele armazena os dados e aguarda que o dispositivo faça contato ao transmitir um comando requisitando os dados. O coordenador envia uma confirmação de recebimento deste comando e envia o quadro de dados. O dispositivo envia uma mensagem de confirmação após receber o quadro.
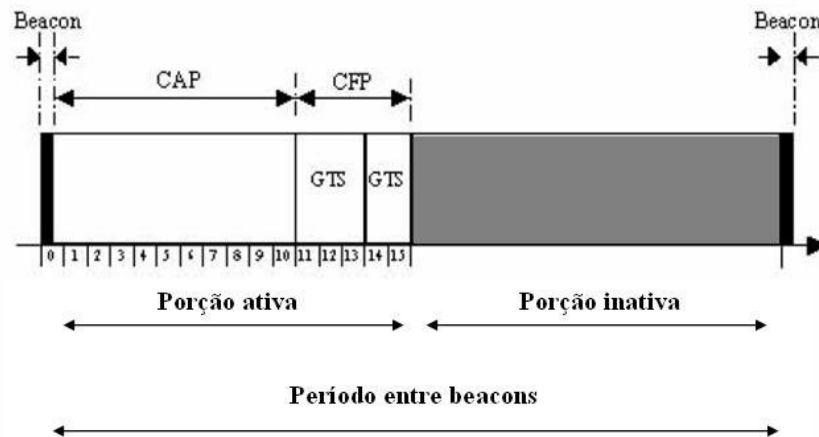
Figura 17 - Estrutura de super-quadro no ZigBee

Um FFD indica sua presença numa PAN transmitindo quadros *beacons*. Isto permite outros dispositivos realizarem a descoberta do dispositivo. Um FFD, que não é o coordenador da PAN, deve iniciar a transmissão de quadros *beacon* apenas quando estiver devidamente associado a uma PAN. O procedimento de associação começa por enviar um comando de solicitação de associação ao coordenador da PAN. O coordenador verifica se é possível associar o dispositivo à rede. Se a resposta for positiva, o coordenador gera um comando de resposta de associação contendo o novo endereço e uma indicação de associação realizada. Esta resposta estará contida em um *beacon* ou será solicitada pelo dispositivo, dependendo do modo de operação da rede.

A sincronização é realizada através dos quadros de sinalização numa rede com *beacons*.

Para redes sem sinalização, esse sincronismo é efetuado ao solicitar dados ao coordenador [20].

O padrão IEEE 802.15.4 emprega um protocolo "*full handshake*" simples para assegurar transferência de dados confiáveis e um bom QoS [21]. Com exceção de quadros de transmissão (p. ex, sinalizadores) e do quadro de reconhecimento, cada quadro recebido pode ser reconhecido para assegurar ao equipamento transmissor que sua mensagem foi de fato recebida. Se um quadro de reconhecimento solicitado não for recebido pelo equipamento transmissor, o quadro pode ser retransmitido.

O padrão 802.15.4 inclui a definição de serviços de segurança fornecidos pela camada MAC. Existem quatro serviços básicos de segurança definidos:

- Controle de acesso – habilita o MAC a selecionar os dispositivos com os quais se deseja comunicar baseado no endereço MAC;
- Criptografia – uso de chave simétrica de criptografia na encriptação de quadros MAC;
- Integridade – permite que o receptor detecte modificações na mensagem usando um código de integridade. Esse código é gerado pela camada MAC e anexado ao quadro MAC;
- *Sequential freshness* – uma seqüência de valores ordenados é anexada ao quadro para prevenir ataques de repetição, no qual mensagens antigas são capturadas por um atacante e reenviadas depois.

Os serviços da camada MAC são usados em várias combinações, baseadas em um dos três tipos de modos de segurança suportados pelo 802.15.4:

- Modo inseguro: nenhuma segurança é fornecida. Os quadros MAC são enviados em texto claro, sem verificação de integridade ou controle de acesso;
- Modo lista de acesso: neste modo o MAC habilita o serviço de controle de acesso, mantendo uma lista com os endereços dos dispositivos com os quais é permitido se comunicar;
- Modo seguro: neste modo o dispositivo pode ter qualquer dos quatro serviços de segurança habilitados, dependendo da segurança implementada.

3.2.3. Camada de rede e camada de aplicação

A camada de rede é a primeira camada realmente definida pelo padrão ZigBee. É de sua responsabilidade: o início ou fim da participação de um dispositivo na rede; a descoberta de novos dispositivos na vizinhança (e o armazenamento das informações relativas aos mesmos); atribuição de endereços (apenas no dispositivo coordenador); descoberta de rotas; encaminhamento de informações e de configuração de novos dispositivos.

A camada de rede do coordenador é responsável por iniciar uma nova rede, e atribuir endereços aos novos dispositivos associados.

Cada quadro NPDU da camada de rede consiste nos seguintes componentes, ilustrados na Figura 18: cabeçalho NWK, contendo controle de quadro, endereçamento e informação de seqüências; e carga NWK, de tamanho variável.

Bytes: 2	2	2	1	1	0/8	0/8	0/1	variável	variável
Controle de quadro	End. destino	End. fonte	Raio	Número de seqüência	End. IEEE Destino	End. IEEE Fonte	Controle multicast	Subquadro de rota	Carga
Cabeçalho NWK									Carga

Figura 18 - Estrutura do quadro na camada de rede do ZigBee

A camada de rede é requisitada a prover funcionalidade para garantir uma correta operação da subcamada MAC do IEEE 802.15.4 e a fornecer uma interface de serviço adequada à camada de aplicação. Para a interface com a camada de aplicação, a camada de rede conceitualmente inclui duas entidades de serviço que fornecem a funcionalidade necessária: a entidade de dados e a entidade de gerenciamento.

A entidade de dados da camada de rede (NLDE – *network layer data entity*) permite que uma aplicação possa transportar APDUs (*application protocol data units*) entre dois ou mais dispositivos na mesma rede. O NLDE oferece os seguintes serviços:

- Gerar PDU em nível de rede (NPDU – *network* PDU), adicionando um cabeçalho apropriado;
- Roteamento, transmitindo a NPDU ao dispositivo apropriado que pode ser o destino final ou o próximo salto na cadeia de comunicação;
- Segurança, com a habilidade de garantir autenticidade e confidencialidade de transmissão.

A entidade de gerenciamento da camada de rede (NLME – *network layer manegement entity*) deve prover os seguintes serviços:

- Iniciar uma rede;
- Participar e deixar uma rede, bem como a habilidade de um coordenador ou *router* de solicitar que um dispositivo deixe a rede;
- Endereçamento: capacidade do coordenador e dos *routers* de atribuir endereços aos dispositivos que se juntem à rede;
- Descoberta de vizinhos, descobrindo, armazenando e reportando informações sobre vizinhos de um salto;
- Descoberta de rotas, descobrindo e armazenando caminhos através da rede para roteamento das mensagens;

- Controle de recepção: capacidade de controlar quando o receptor está ativo e por quanto tempo.

A camada de aplicação contém a subcamada APS (*application support*), o ZDO (ZigBee *device object*) e o *framework* da aplicação.

A camada APS faz o roteamento das mensagens aos diferentes pontos da aplicação que funcionam no nó. Isto inclui manter as tabelas de *binding* (tabela que mantém as conexões compatíveis entre diferentes *endpoints*).

No topo da pilha estão os objetos das aplicações, sendo cada um deles um *software* em um *endpoint*, que executa o que o dispositivo é projetado fazer. São desenvolvidos pelos produtores das aplicações e se comunicam através das funções disponibilizadas pela camada APS.

As responsabilidades da subcamada APS incluem:

- Manter tabelas de *binding*, definido como a habilidade de combinar dois dispositivos baseado nos seus serviços e necessidades;
- Repassar mensagens entre dispositivos “ligados” pela tabela de *binding* [25];
- Definição de endereço de grupos, remoção e filtragem de mensagens endereçadas a grupos;
- Mapeamento dos endereços de 64 *bits* do IEEE de e para endereços de 16 *bits* da camada de rede;
- Fragmentação, rearranjo e confiabilidade de dados de transporte [25].

Cada quadro APS da camada de aplicação tem a estrutura apresentada na Figura 19: cabeçalho APS, contendo controle de quadro e informações de endereço; e carga APS, de tamanho variável.

Bytes:1	0/1	0/2	0/2	0/2	0/1	1	variável
Controle de quadro	Endpoint de destino	End. de grupo	Identificador de cluster	Identificador de perfil	Endpoint da fonte	Contador APS	Carga
	Campos de endereçamento						
Cabeçalho APS							Carga APS

Figura 19 - Estrutura do quadro APS do ZigBee

A subcamada APS provê uma interface entre a camada de rede e a camada de aplicação através de um conjunto de serviços usados tanto pelo ZDO quanto pelos objetos definidos pelo fabricante. Os serviços são fornecidos por duas entidades: a entidade de dados APS (APSDE) e a entidade de gerenciamento APS (APSME).

O APSDE fornece serviço de transmissão de dados para o transporte de PDUs de aplicação entre dois ou mais dispositivos. O APSME provê serviços de segurança, *binding* de dispositivos,

estabelecimento e remoção de endereços de grupos e também mantém uma base de dados dos objetos gerenciados. Essa base de dados dá suporte ao mapeamento entre endereços de 64 bits do IEEE e de 16 bits da camada de rede.

O ZDO (*ZigBee device objects*) está localizado entre o *framework* da aplicação e a subcamada APS. Representa uma classe de funcionalidades que provêem uma interface entre os objetos da aplicação, o perfil de dispositivo e a subcamada APS. Satisfaz exigências comuns de todas as aplicações operando na pilha ZigBee.

O ZDO é como um objeto de aplicação especial, que é residente em todos os nós da rede ZigBee. É sempre o *endpoint* zero, e os outros *endpoints* são numerados de 1 a 240. Tem seu próprio perfil, conhecido como o perfil do dispositivo ZigBee (ZDP), que tanto os outros *endpoints* quanto os outros nós da rede podem alcançar. É o ZDP que contém os serviços para a descoberta do dispositivo. O ZDO é então responsável pela gerência do dispositivo total e também por chaves e políticas de segurança. As aplicações fazem chamadas ao ZDO a fim de descobrir outros dispositivos ZigBee na rede e os serviços que oferecem, e especificar ajustes da segurança e da rede.

As responsabilidades do ZDO incluem:

- Definir o papel do dispositivo na rede (coordenador, *router* ou *endpoint*);
- Iniciar e/ou responder às requisições de *binding*;
- Estabelecer uma relação segura entre dispositivos.

O ZDO também é responsável por descobrir dispositivos na rede e determinar quais serviços de aplicação eles dispõem [25]. A descoberta de dispositivos é o processo onde um dispositivo ZigBee pode descobrir outros dispositivos iniciando perguntas. Há duas formas de solicitação de descoberta: requisição de endereço IEEE e requisição de endereço de rede. A requisição de endereço IEEE é direcionada e assume que o endereço de rede é conhecido. A requisição de endereço de rede é feita por *broadcast* e carrega o endereço IEEE conhecido no campo de carga. Dispositivos do tipo *router* ou coordenador respondem a uma requisição de endereço de rede enviando seu endereço de rede e o endereço de rede dos dispositivos a eles associados [25].

O *framework* de aplicação no ZigBee é o ambiente no qual os objetos da aplicação estão localizados nos dispositivos ZigBee. Dentro do *framework*, os objetos enviam e recebem dados através do APSDE. Há 240 objetos distintos que podem ser definidos, cada um conectado a um *endpoint* indexado de 1 a 240. Dois *endpoints* adicionais são definidos para uso do APSDE: o *endpoint* 0 é reservado para o ZDO e o *endpoint* 255 é reservado para função de *broadcast*. Os e*ndpoints* 241 a 254 são reservados para uso futuro [25].

Um conceito central na camada de aplicação ZigBee é o perfil de aplicação. Os perfis de aplicação definem os dispositivos, mensagens e ações de processamento que constituem uma

aplicação sendo executada entre *end devices* em um determinado ambiente, de forma a garantir compatibilidade e interoperabilidade entre eles. Há um campo Identificador de Perfil no quadro da camada de aplicação que especifica o perfil. De potencial interesse para a automação industrial e de processos é o perfil IPM (*Industrial Process Monitoring*), que está sendo desenvolvido pela ZigBeee Alliance e irá prover um conjunto de descrições de dispositivos e formatos de mensagens relacionadas ao monitoramento e controle de equipamentos (por exemplo, sensores de temperatura e pressão e seus respectivos parâmetros e valores de saída) [23].

4. Interconexão entre redes *fieldbus* e redes sem fio

Devido às propriedades especiais da transmissão sem fio, não é desejável que todos os nós de uma rede industrial de comunicação sejam sem fio [11]. A necessidade de adaptar os sistemas existentes com suporte para a tecnologia sem fio, ao invés de criar novos sistemas, aumenta o desejo por redes *fieldbus* híbridas [35]. Os protocolos utilizados em sistemas cabeados não são projetados para um meio sem fio, devendo ser substituídos por protocolos adaptados nos enlaces sem fio, não devendo ser necessário modificar a pilha de protocolos das estações cabeadas. Além do mais, os dispositivos cabeados precisam se comunicar com os nós sem fio, trazendo a necessidade de formas de interconexão. Entretanto, as diferenças entre as propriedades de transmissão com e sem fio introduzem dificuldades a esta convivência. Estas dificuldades são agravadas pelas necessidades especiais existentes nas redes de campo industriais.

A informação que trafega em ambientes industriais é tipicamente informação de estado/situação e em operação normal toma a forma de “rajadas” repetidas de pequenos pacotes. Ao mesmo tempo, estes pacotes estão associados com tarefas críticas possuindo requisitos de tempo restritos em ambientes hostis. Assim, em geral, a taxa de transferência de dados da rede é relativamente baixa, mas sua confiabilidade precisa ser muito alta [35]. Nos sistemas *fieldbus* em que os pacotes são transmitidos para uma estação com endereço explícito, a confiabilidade pode ser aumentada através de diversos mecanismos, como retransmissão, duplicação de pacotes ou códigos corretores de erros. Por outro lado, em sistemas de tipo produtor-consumidor, em que os dados são transmitidos em *broadcast* e as estações interessadas copiam estes dados, tais mecanismos não são usados. Geralmente, os dados são transmitidos periodicamente e as perdas são detectadas ao comparar o período conhecido e o instante de chegada do último pacote [10]. Esta informação é usada pela aplicação para agir apropriadamente.

Requisitos importantes que devem ser preservados em sistemas industriais de comunicação para a realização da interconexão [11]:

- Manipular tráfego periódico com diferentes períodos, sendo capaz de transportar a informação antes do fim do período em que o dado é amostrado;
- Manipular tráfego aperiódico com latência delimitada;
- Permitir consulta em tempo real de um número de entradas em diferentes nós da rede;
- Para dados esporádicos, prover formas de saber a ordem em que os eventos ocorreram;
- Transferir dados de um nó para outro nó, ou para vários nós.

Segmentos cabeados e sem fio são acoplados com o uso de dispositivos acopladores. Um

segmento é definido como um conjunto de estações ligadas a um meio comum, que rodam os mesmos protocolos e concordam nos parâmetros de transmissão, sendo assim capazes de se comunicar diretamente [38]. Em redes sem fio, os segmentos são denominados de células [11].

Os dispositivos usados no acoplamento podem ser: repetidores, pontes ou *gateways*.

Uma solução de interconexão baseada em repetidores dá a impressão que todos os nós compartilham o mesmo meio. O mesmo mecanismo de controle de acesso ao meio é usado na parte cabeada e na parte sem fio. Repetidores operam sobre a camada física. Convencionalmente, eles trabalham bit por bit recebendo o sinal de entrada, regenerando o sinal e emitindo-o do outro lado [2]. No contexto de repetidores localizados entre segmentos e células, isto implica em mudanças no esquema de codificação. Entretanto, teoricamente, os repetidores são transparentes para os protocolos acima da camada física. Como a transmissão sem fio está mais susceptível a erros, um tipo diferente de repetidor pode ser usado. Ao invés de repetir o sinal *bit* por *bit*, o repetidor de palavras espera que certo número de bits chegue do lado cabeado, calcula um código de correção de erros, e transmite os bits da informação junto com o código corretor [11]. Ao receber dados do lado sem fio, o repetidor usa o código corretor para corrigir possíveis erros e retransmite os bits de informação, possivelmente corretos, no segmento cabeado. Este tipo de repetidor introduz um atraso longo, contudo menor que o atraso de uma ponte ou *gateway* [11].

Se as taxas de bits nos dois lados do repetidor forem diferentes, o repetidor precisa armazenar a informação. A política de armazenamento irá diferir dependendo da direção da informação. Para transmitir do lado mais rápido para o mais lento, é necessário armazenar os bits que chegam antes de emiti-los do outro lado. Se a retransmissão ocorre em sentido contrário, é preciso esperar por uma quantidade suficiente de bits para emitir o pacote completo no lado mais rápido. Isto significa que o repetidor deve conhecer o tamanho máximo do pacote.

Como possíveis colisões na parte sem fio não podem ser detectadas durante a transmissão, existem restrições quanto ao tipo de protocolo de acesso ao meio que será usado na camada de enlace. Os protocolos com detecção de colisão não podem ser usados diretamente.

Na presença de um grande número de nós, o uso de repetidores pode ocasionar períodos ou latências inaceitáveis. Ao usar uma ponte, os nós serão divididos em dois segmentos. No caso em que uma maior parte do tráfego permanece em cada segmento (ou célula) e o tráfego entre segmentos é mínimo, a solução baseada em ponte oferece significativa redução na latência se comparada com a solução baseada em repetidores [11]. Uma ponte atua na camada de enlace, recebendo um quadro MAC completo, verificando-o e possivelmente repassando o quadro no outro lado. Pontes conversoras (*translation bridges*) são usadas quando ambas as redes possuem endereçamento e funções da camada de enlace suficientemente parecidas que permitam uma conversão direta dos PDUs entre as duas redes. Pontes de encapsulamento (ou tunelamento) devem ser usadas quando a conversão não é possível. O quadro é encapsulado no formato da rede de

destino antes de ser repassado.

Há, portanto, um tempo de espera antes de emitir o quadro na rede de destino, que depende do protocolo MAC. Em geral, o uso de pontes requer que as camadas superiores sejam idênticas em ambos os lados [11]. Uma ponte participa como um nó em ambas as redes.

Gateways são úteis quando o segmento cabeado e a célula sem fio são construídos com protocolos não compatíveis na camada de enlace. Por exemplo, um protocolo baseado no modelo cliente-servidor não inclui a mesma informação que um protocolo baseado no modelo produtor-consumidor. O primeiro inclui os endereços dos nós de fonte e de destino. O segundo inclui apenas a identificação dos dados. Não é possível usar uma ponte. Os g*ateways* atuam na camada de aplicação, e também são necessários quando as camadas de aplicação dos segmentos diferem entre si. Quando um *gateway* recebe alguma indicação de serviço de aplicação, esta é convertida em uma requisição de serviço na rede de destino. Quando a confirmação é recebida, o *gateway* repassa-a como uma resposta no outro lado. Soluções baseadas em *gateways* possuem, em geral, latências maiores do que soluções com pontes, devido aos cabeçalhos adicionais introduzidos pelas camadas superiores. Uma solução interessante é ter um *gateway* atuando como *proxy*. O objetivo é superar o atraso adicional realizando solicitações antecipadamente. O *gateway* responde a um dos lados como se fosse um nó da outra rede, guardando uma imagem dos dados de todas as estações de um dos lados. Ao receber uma solicitação de serviço, o valor armazenado é retornado como resposta. O *gateway*, então, atua como uma estação-base para a célula, representando os nós sem fio no segmento cabeado.

Além da preocupação com o dispositivo de acoplamento, é fundamental observar o processo de encaminhamento das mensagens. Redes de comunicação utilizam endereços para identificar as estações e assim encaminhar mensagens a estas. Existem duas possibilidades de como entregar um pacote de um nó em uma rede para um nó em outra rede com esquemas de endereçamento diferentes:

A. Um endereço virtual da rede de origem é atribuído ao nó de destino pertencente à outra rede;
B. O nó fonte envia o pacote ao dispositivo acoplador, e este entrega o pacote ao nó de destino.

No primeiro esquema o nó fonte não faz distinção quanto ao protocolo do companheiro, ou seja, a interconexão é transparente [31]. Já no segundo caso ocorre o oposto.

O atraso introduzido pelos acopladores é importante. Em repetidores e em certos tipos de pontes, os pacotes são repassados de um segmento para outro sem modificações em seus conteúdos ou com pequenas modificações (por exemplo, uma mudança no formato do endereçamento). O atraso de retransmissão no acoplador pode ser definido como o intervalo de tempo entre o instante em que o último bit do pacote é recebido do segmento de origem e o instante em que o último bit do

pacote é transmitido no segmento de destino [10].

A diferença entre os tamanhos dos campos de carga das duas redes também deve ser considerada. Um método trata o problema fazendo com que o acoplador fragmente e rearranje pacotes, de acordo com o sentido da comunicação, para preencher a diferença. Outro método adotado é que os nós devem ser projetados para evitar qualquer fragmentação ou rearranjo.

A escolha da solução de interconexão depende dos protocolos usados, tipos de garantias oferecidas e restrições, especialmente as relacionadas ao tempo. Em geral, quanto mais baixa a interconexão no modelo OSI, melhores são as performances [11]. Mas é preciso verificar cuidadosamente cada caso em particular.

O cenário proposto é interligar uma rede de dispositivos sem fio ZigBee à redes PROFIBUS e FOUNDATION Fieldbus. A rede de sensores é composta de sensores e atuadores que atuam em um determinado processo presente na planta industrial. Esta rede será denominada de segmento sem fio, rede ZigBee ou célula ZigBee.

Uma das duas redes de campo executa a comunicação entre a rede ZigBee e os demais dispositivos presentes no sistema: instrumentos de campo e terminais de controle, supervisão ou configuração. As duas seções a seguir tratam com mais detalhes os aspectos observados na tentativa de implementação do cenário proposto nos casos citados.

4.1. PROFIBUS + ZigBee

A idéia proposta para a interconexão de uma rede de sensores e atuadores ZigBee com uma rede PROFIBUS é utilizar a célula ZigBee em áreas classificadas, substituindo um segmento PROFIBUS PA. O cenário é apresentado na Figura 20.
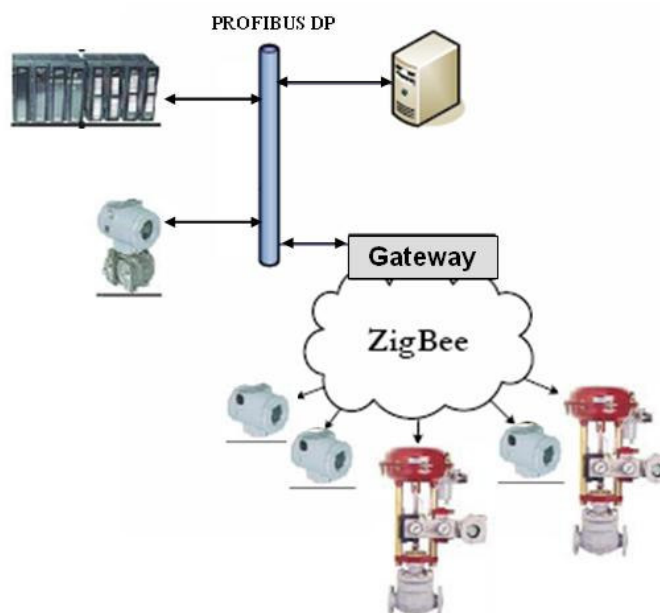
Figura 20 - Cenário proposto para interconexão entre uma rede PROFIBUS e uma célula ZigBee

O acoplamento entre os dois segmentos acontece de forma similar ao realizado por um dispositivo tipo *Link* DP/PA apresentado na seção 2.1.1. Desta forma, o dispositivo de acoplamento possui um endereço no segmento PROFIBUS DP e os nós da rede ZigBee são relacionados a este único endereço no segmento, não reduzindo a capacidade de endereçamento, que é limitada a 126 endereços no segmento DP. Os nós ZigBee são alcançados por um mestre na rede DP da mesma forma que um dispositivo com perfil PA seria alcançado. A diferença é que a conversão não ocorre apenas na camada física ou de enlace, mas até a camada de aplicação, já que o acoplamento é feito por um *gateway*. O uso do *gateway* é necessário porque as camadas de enlace nas redes PROFIBUS e ZigBee são diferentes. Além disso, a pilha de protocolos ZigBee contém a camada de rede, não inclusa em redes PROFIBUS.

Para realizar a conversão dos endereços entre as redes, o *gateway* mantém uma tabela contendo a associação entre os endereços na rede PROFIBUS e os endereços correspondentes na rede ZigBee, já que os mesmos possuem comprimentos distintos.

Um aspecto importante que deve ser observado na construção de redes ZigBee interligadas a uma rede PROFIBUS é o requisito de tempo (latência) de algumas aplicações. O PROFIBUS DP utiliza um mecanismo de passagem de *token* entre os mestres presentes no barramento. Quando o mestre possui o *token* ele está apto a se comunicar com seus escravos através de solicitações. O tempo de posse do *token* é especificado na configuração do sistema. Uma rede ZigBee, assim como outras redes de comunicação sem fio, está mais sujeita a interferências provenientes do meio de transmissão do que redes cabeadas. Consequentemente, o número de retransmissões aumenta, resultando em maiores latências. Este fato, associado à limitação de tempo de posse do *token* por um mestre, prejudica a performance do sistema. A primeira solução seria aumentar o tempo de posse do *token*, porém outras aplicações críticas existentes no sistema seriam afetadas.

Uma alternativa é usar um *gateway* que atue como *proxy*. Assim o *gateway* armazena as informações dos nós ZigBee e responde às solicitações provenientes de um mestre na rede DP. Do lado da rede sem fio, a consulta aos dados dos dispositivos obedece a um dos mecanismos disponíveis no ZigBee. O *gateway* é o coordenador na rede ZigBee. Operar no modo com sinalização (modo com *beacon*) usando uma estrutura de super-quadro é mais atrativa, pois além de possibilitar baixo consumo de energia nas estações, também permite que os dispositivos utilizem o período sem disputa CFP da porção ativa do super-quadro para realizar comunicações periódicas. As demais estações fazem uso dos períodos com disputa CSMA/CA com *time slots* (período CAP da porção ativa) ou sem *time slots* (porção inativa). Outro benefício é que o uso de *beacons* proporciona uma melhor sincronização na rede ZigBee. O período entre *beacons* deve ser suficiente para que as estações realizem a comunicação necessária com o coordenador, mas esse intervalo não deve ultrapassar o tempo de rotação do *token*. Assim, as chances dos dados armazenados no *cache*

do *gateway* serem atuais aumentam, uma vez que os dados das estações ZigBee serão atualizados antes da próxima solicitação realizada pelo mesmo mestre.

Outro aspecto relevante é o tamanho dos pacotes que circulam nas duas redes em questão. Em uma rede PROFIBUS a carga útil trocada entre dispositivos ocupa no máximo 246 *bytes*. Já numa rede ZigBee esse comprimento é reduzido para 102 *bytes*. Existem duas possibilidades: na primeira o *gateway* é responsável por fragmentar os pacotes antes de enviá-los a estação sem fio; na segunda opção a aplicação no dispositivo PROFIBUS delimita o tamanho da carga útil a ser enviada. A segunda alternativa é mais atraente, já que na primeira seria preciso dotar os dispositivos ZigBee de capacidade de ordenação dos pacotes fragmentados, o que resultaria em maior processamento, aumentando os custos e o consumo de energia. A limitação de tamanho dos pacotes pode ser realizada durante a configuração da rede PROFIBUS.

4.2. FOUNDATION Fieldbus + ZigBee

A utilização de uma rede FOUNDATION Fieldbus no cenário ilustrado na Figura 21 é semelhante à descrita na seção anterior. Entretanto, devido às diferenças existentes entre PROFIBUS e FOUNDATION Fieldbus, são necessárias algumas observações.
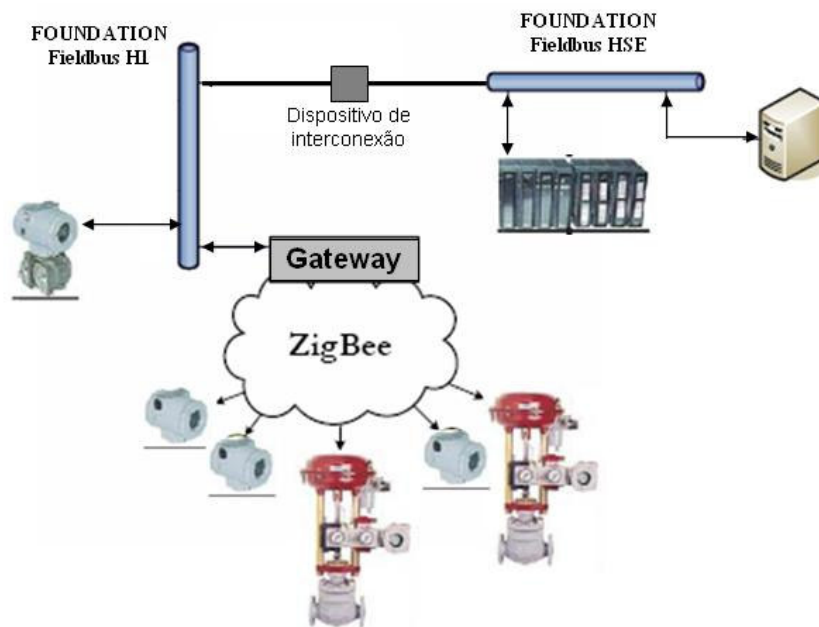
Figura 21 - Cenário proposto para interconexão entre FOUNDATION Fieldbus e ZigBee

Assim como no caso anterior, um *gateway* é o dispositivo responsável pelo acoplamento entre as redes FOUNDATION Fieldbus e ZigBee, já que os protocolos usados nas camadas de enlace são diferentes. O *gateway* realiza a conversão de endereço e formato dos quadros entre a rede FOUNDATION Fieldbus H1 e a célula de dispositivos sem fio. Neste caso a rede de dispositivos ZigBee substitui instrumentos H1 que seriam conectados a um *hub* no barramento.

Um segmento H1 permite endereçar até 240 dispositivos. Além disso, existe um campo reservado para o endereço do segmento. Desta forma, um dispositivo é identificado por um endereço de segmento e um endereço de nó. Na rede híbrida proposta, a célula ZigBee é identificada por um endereço de segmento na rede H1, e cada estação sem fio tem um endereço de nó correspondente no barramento H1. Todas as mensagens endereçadas a uma estação na célula ZigBee são capturadas pelo *gateway* que mantém uma tabela de associação entre os endereços H1 e os endereços ZigBee. O *gateway* é responsável por encaminhar a mensagem ao nó sem fio correspondente. O endereço de segmento é interpretado pelas estações ZigBee como um identificador de PAN, e seu uso auxilia o *gateway* na identificação do destino das mensagens recebidas em ambos os lados.

A comunicação numa rede H1 pode ocorrer de forma agendada ou não-agendada. Assim, os nós na célula ZigBee podem ser requisitados de ambas as formas, a depender da aplicação em uso. Devido as propriedades do meio de transmissão sem fio, é interessante que o *gateway* represente as estações sem fio na rede FOUNDATION Fieldbus, exercendo uma função de *proxy*. O objetivo é não prejudicar o desempenho da rede de campo. Se uma das estações ZigBee estiver na lista de comunicação agendada, o *gateway* intercepta a mensagem CD (*compel data*) e realiza a publicação das informações contidas em seu *cache* referentes à estação ZigBee correspondente. Se uma estação sem fio estiver contida na "*live list*", mais uma vez o *gateway* será o intermediador, recebendo o PT (*pass token*) e transmitindo os dados referentes à estação ZigBee apropriada.

As informações dos dispositivos sem fio, armazenadas no *cache* do *gateway*, são atualizadas usando o modo de operação com sinalização numa estrutura de super-quadro com porção ativa e inativa. As razões são as mesmas apresentadas na seção anterior: possibilidade de tratar dados periódicos e aperiódicos, e maior sincronização na rede ZigBee. O intervalo entre *beacons*, que caracteriza os períodos das porções ativa e inativa, deve ser condizente aos intervalos de comunicação na rede H1.

A diferença entre os tamanhos dos pacotes que circulam nas duas redes é um aspecto importante. A carga útil numa rede H1 tem comprimento máximo de 251 *bytes*. Enquanto que na rede ZigBee não pode ultrapassar 102 *bytes*. A possibilidade de fragmentação no *gateway* é descartada, pois exige maior capacidade de processamento e consumo de energia nas estações sem fio. Resta então limitar o comprimento da carga útil na rede H1 durante a configuração do sistema.

4.3. Conclusões

Em ambas as propostas de solução apresentadas, a célula ZigBee substitui uma ramificação da rede industrial, que seria usada para conectar os dispositivos de campo atuantes em um determinado processo. O principal objetivo é eliminar o uso de cabos para comunicação, permitindo maior flexibilidade e redução de custos. O emprego da tecnologia ZigBee restringiu-se a células em

processos isolados para limitar o raio de alcance das mesmas. Com isso, é possível confinar as informações trocadas via rádio ao setor industrial, dificultando a detecção ou invasão por estranhos. Por essa mesma razão, é possível usar uma topologia em estrela na célula ZigBee, com as estações sendo dispositivos do tipo RFD, ocasionando uma maior redução de consumo de energia nas estações.

Quanto aos prováveis prejuízos no desempenho das redes *fieldbus*, o uso de um *gateway proxy* é capaz de atender as necessidades dos mecanismos de acesso ao meio, tanto no PROFIBUS quanto no FOUNDATION Fieldbus. Além do mais, a taxa de transferência em uma rede ZigBee é 250 kbps (na freqüência 2,4 GHz), enquanto que em redes PROFIBUS PA e FOUNDATION Fieldbus H1 é 31,25 kbps.

Ao receber dados provenientes da rede *fieldbus* com destino à rede sem fio, o *gateway* desencapsula o quadro à medida que este ascende na pilha de camadas, retirando os campos inseridos pela camada par na estação de origem. O campo de dados de usuário é retirado, e inserido no campo de dados ZigBee, no topo da pilha de protocolos. Uma vez que o tamanho dos dados foi limitado durante a configuração do sistema não é preciso preocupar-se quanto à fragmentação. Os campos contendo as informações de endereços são usados pelo *gateway* para consultar a tabela de conversão de endereços, e assim efetuar corretamente o envio da mensagem na rede sem fio. Processo semelhante é realizado quando o *gateway* recebe uma mensagem vinda da rede ZigBee com destino à rede cabeada *fieldbus*.

Para prover conectividade com as redes PROFIBUS DP e FOUNDATION Fieldbus H1, o *gateway* deve possuir um conector apropriado para a tecnologia de transmissão selecionada (RS485, IEC 61158-2 ou fibra ótica). Deve suportar taxas de transmissão que variam de 9,6 kbps a 12 Mbps no caso de uma rede PROFIBUS DP, ou uma taxa de 31,25 kbps quando for utilizado em uma rede FOUNDATION Fieldbus H1.

Além da conexão com a respectiva rede *fieldbus*, o *gateway* contém circuitos de transmissão/recepção capazes de operar em 2,4 GHz para a comunicação no enlace sem fio. Neste caso, utiliza-se a técnica DSSS com modulação O-QPSK, abrangendo 16 canais. A potência de transmissão dependerá do alcance que se deseja obter, e a sensibilidade de recepção será -85 dBm. A taxa de transmissão de dados na rede ZigBee deve ser projetada para alcançar 250 kbps.

O *gateway* deve possuir capacidade de processamento que atenda a execução de suas funcionalidades, dentro do menor tempo possível. Outro aspecto importante é a quantidade de memória disponível, sendo necessários dois tipos de memória: uma não-volátil para guardar as configurações do equipamento e as tabelas de associação de endereços; e uma memória volátil que auxilie na execução das tarefas e contenha o *cache* com os dados das estações.

Caso não seja possível implementar uma das duas soluções propostas, especialmente devido ao projeto do *gateway proxy*, pode-se lançar mão de outra alternativa para a interconexão de

células ZigBee às redes PROFIBUS e FOUNDATION Fieldbus. Existem técnicas [31, 32 e 33] para a realização da interconexão de uma rede ZigBee com uma rede IP. Conforme descrito na seção 2.1.4, o PROFINET é uma solução baseada em IP capaz de interligar redes PROFIBUS. Já o HSE, apresentado na seção 2.2.2 é usado na conexão de diversos segmentos H1 nas redes da Fieldbus Foundation, e também possui uma pilha de protocolos TCP/IP. Sendo assim, a célula ZigBee poderia estar interligada ao sistema *fieldbus* por meio destas soluções. A dificuldade está na implementação desta opção em plantas que já possuem uma estrutura montada, seja em PROFIBUS ou FOUNDATION Fieldbus. O aproveitamento do arranjo existente pode ser mais atrativo do que uma reestruturação.

5. Conclusão

As redes de campo industriais vêm exercendo papel de destaque na automação, especialmente no setor de processos. O uso das denominadas redes *fieldbus* tem aumentado nos últimos anos, com destaque para as redes PROFIBUS e FOUNDATION Fieldbus. Estas possuem a características de serem sistemas abertos, que facilitam a convivência entre dispositivos de fabricantes distintos em uma mesma rede de comunicação.

Outro ramo das tecnologias de comunicação também merece atenção: a transmissão sem fio, particularmente através de ondas de rádio. Os investimentos em pesquisas têm incentivado o uso dos mais diversos padrões relacionados a esta tecnologia. O setor industrial não foge à regra.

Sistemas com fio são caros e mais caro ainda é modificar o *layout* de uma instalação. Sistemas sem fios resolvem estes problemas, e o padrão ZigBee tem particularidades que o tornam atrativo para aplicações industriais. A alta densidade de nós e o baixo consumo de energia são as características mais marcantes do ZigBee.

Há uma tendência para dispor as redes de campo industriais atualmente em operação com capacidades de comunicação sem fio, levando às redes híbridas. O objetivo primário de sistemas *fieldbus* é prover comunicação em tempo real, com garantias de tempo e de entrega de pacotes. Rodar aplicações baseadas em *fieldbus* com tecnologias sem fio pode ser especialmente desafiador. Como os canais sem fio estão mais susceptíveis a erros durante a transmissão, os requisitos de confiabilidade e tempo real estão mais ameaçados do que estariam se a informação trafegasse através de cabos. Ações que podem reduzir esses problemas:

- Selecionar a banda menos susceptível a interferências;
- Configurar os dispositivos para usarem um determinado canal na banda escolhida, o canal que seja menos afetado;
- Aumentar a potência do sinal de transmissão ao selecionar produtos com níveis melhores ou antenas com ganhos maiores;

Outro aspecto relevante é que a segurança não exerce papel importante no desenvolvimento de padrões *fieldbus* [10]. Como a informação trafega dentro de cabos, uma possível intrusão só acontece através de acesso aos terminais, ou violando o cabeamento. Entretanto, a introdução de meios sem fio permitiu que um atacante pudesse capturar pacotes a certa distância. Pior que isso, um atacante pode gerar interferências na freqüência de operação ou introduzir pacotes maliciosos na rede. Sendo assim, medidas de segurança (integridade, autenticidade, autorização) têm que ser adicionadas a sistemas *fieldbus* sem fio.

Em se tratando da interação entre redes *fieldbus* e redes sem fio, duas situações foram investigadas neste trabalho. O primeiro cenário avaliado foi a integração entre um segmento

ZigBee, denominado de célula ZigBee, e uma rede PROFIBUS. A idéia é substituir um segmento com dispositivos do perfil PROFIBUS PA, atuante em um processo, por uma célula ZigBee. Esta última seria diretamente conectada a um barramento PROFIBUS DP por meio de um *gateway*. Além de ser responsável por converter os formatos dos quadros e endereços diferentes entre as redes, o *gateway* também atua como *proxy* para que o desempenho do mecanismo de acesso ao meio no PROFIBUS não seja prejudicado.

O segundo cenário investigado contempla a interconexão entre uma célula ZigBee e um barramento FOUNDATION Fieldbus H1. O objetivo é semelhante ao caso anterior. Também existe a presença do *gateway proxy*, capaz de armazenar as informações das estações sem fio em *cache*, facilitando a consulta por parte de dispositivos na rede FOUNDATION Fieldbus.

Em ambos os cenários é preciso garantir que, durante a configuração do sistema, os parâmetros de tempo de uma rede atendam os requisitos da outra rede. Além disso, é preciso limitar o tamanho dos pacotes originados nas redes *fieldbus* com destino à célula ZigBee.

A existência das redes híbridas apresentadas é possível, porém não trivial. O projeto do *gateway* exige um estudo detalhado sobre sua capacidade de armazenamento e processamento, podendo, inclusive, não ser economicamente viável a construção do mesmo. Uma alternativa seria utilizar *gateways* ZigBee para redes IP, e conectar a célula sem fio ao PROFINET e ao HSE, respectivamente as soluções baseadas em IP do PROFIBUS e da Fieldbus Foundation. Um ponto negativo é que, desta forma, nem todas as estruturas em funcionamento seriam aproveitadas para a adaptação ao ZigBee.

Dentre os dois cenários expostos, o uso do ZigBee em conjunto com o FOUNDATION Fieldbus é o que reúne mais aspectos favoráveis. Em primeiro lugar, o número de endereços possíveis no segmento H1 é maior que no PROFIBUS DP. Além disso, existe a presença explícita de um campo para o endereço de segmento, capaz de aumentar essa capacidade de endereçamento. A velocidade de transmissão no segmento H1 é única, não sendo necessário dotar o *gateway* de mecanismos de seleção dessa taxa, que pode assumir diversos valores no PROFIBUS DP. A comunicação agendada é garantida com o uso de *slots* reservados na estrutura de super-quadro do ZigBee. Já as informações que trafegam sem agendamento podem utilizar os períodos CSMA/CA de disputa ao canal de comunicação.

Apesar do emprego de tecnologia de comunicação sem fio almejar a eliminação de cabeamento, a ausência completa de cabos pode não ser alcançada. Em termos de tráfego de informação, a inexistência de cabeamento é conseguida, porém ainda há a dependência do uso de fios para a rede elétrica. Mesmo com o aproveitamento de baterias para a alimentação elétrica dos instrumentos na célula ZigBee, alguns dispositivos exigem um alto consumo de energia (ex. atuadores de grande porte), dificultando o uso das baterias. Mesmo assim, a redução de cabos obtida com a utilização de tecnologias sem fio é cobiçável.

Para que se possam validar as conclusões obtidas, se faz necessário lançar mão de atividades experimentais que agreguem as associações analisadas ao longo deste documento. Desta forma, será possível investigar todas as características, restrições e desempenhos de cada um dos cenários propostos. Tais implementações podem ser alvo de trabalhos futuros, com o objetivo de sedimentar e complementar as informações expostas até o presente momento, incorporando novos resultados e conhecimentos.

Referências bibliográficas

[1] MORAES, C. C. e CASTRUCCI, P. L. **Engenharia de automação industrial**. 2ª Ed. Rio de Janeiro: LTC, 2007.

[2] TANENBAUM, A. S. **Redes de computadores**. Trad. de Vandenberg D. de Souza. Rio de Janeiro: Elsevier, 2003.

[3] SEIXAS FILHO, C. **A automação nos anos 2000: uma análise das novas fronteiras da automação**. CONAI, 2000. Disponível em: http://www.cpdee.ufmg.br/~seixas/PaginaII/Download/DownloadFiles/Conai2000Automacao.pdf. Acesso em: 01 de out. 2007.

[4] MIYAGI, P.E. e VILLANI, E. Mecatrônica como solução de automação. **Revista Ciências Exatas**. Taubaté, v.9/10, n. 1-2, p. 53-59, 2003/2004.

[5] SILVA JÚNIOR, W. M. **Gestão para mudança do paradigma tecnológico no controle de processo da RLAM: do 4-20 mA analógico para redes de comunicação digital fieldbus**. Cad. Pesq. NPGA, Salvador, v. 3, p. 1-16, maio - ago. 2006.

[6] SAUTER, T. Fieldbus systems: history and evolution. In: ZURAWSKI, R. (Ed.). **The industrial communication technology handbook**. CRC Press, 2005.

[7] JECHT, U., STRIPF, W. e WENZEL, P. PROFIBUS: open solutions for the world of automation. In: ZURAWSKI, R. (Ed.). **The industrial communication technology handbook.** CRC Press, 2005.

[8] CAVALIERI, S. FOUNDATION Fieldbus: history and features. In: ZURAWSKI, R. (Ed.). **The industrial communication technology handbook.** CRC Press, 2005.

[9] MATHEUS, K. Wireless local and wireless personal area network technologies for industrial deployment. In: ZURAWSKI, R. (Ed.). **The industrial communication technology handbook**. CRC Press, 2005.

[10] WILLIG, A. Wireless LAN technology for the factory floor: challenges and approaches. In: ZURAWSKI, R. (Ed.). **The industrial communication technology handbook**. CRC Press, 2005.

[11] DECOTIGNIE, J-D. Interconnection of wireline and wireless fieldbuses. In: ZURAWSKI, R. (Ed.) **The industrial communication technology handbook**. CRC Press, 2005.

[12] CASSIOLATO, C., TORRES, L. H. B. e CAMARGO P. R. **PROFIBUS – descrição técnica.** Associação PROFIBUS, 2006.

[13] PAZOS, F. **Automação de sistemas e robótica**. Axcel Books do Brasil, 2002.

[14] ACROMAG INCORPORATED. **Technical reference: introduction to PROFIBUS DP**. 2002.

[15] SAMSON AG. **Technical information: PROFIBUS-PA**. 1999.

[16] SMAR INTERNATIONAL. **FOUNDATION Fieldbus tutorial.** Disponível na Internet. Http://www.smar.com/PDFs/catalogues/FBTUTCE.pdf. Acesso em: 03 de dez. 2007.

[17] SAMSON AG. **FOUNDATION Fieldbus – Technical information.** Maio 2000. Disponível na Internet. Http://www.samson.de. Acesso em: 15 de dez. 2007.

[18] Yokogawa Electric Corporation. **Fieldbus Book – A tutorial.** Maio 2001. Disponível na Internet. http://www.algumacoisa.com. Acesso em: 17 de dez. 2007.

[19] NATIONAL INSTRUMENTS. **Foundation Fieldbus overview**. 2003.

[20] ERGEN, S. C. **ZigBee/IEEE 802.15.4 summary**. 2004

[21] GESSINGER, A. K. e HENNIG, C. H. **ZigBee – conectividade wireless para automação e controle**. 200?.

[22] MALAFAYA, H., TOMÁS, L. e SOUSA, J.P. **Sensorização sem fios sobre ZigBee e IEEE 802.15.4**. Porto, Portugal: 200?.

[23] MASICA, K. **Recommended practices guide for securing ZigBee wireless networks in process control system environments**. Califórnia, EUA: 2007.

[24] CRAIG, W. C. **ZigBee: wireless control that simply works**. ZigBee Alliance. 200?.

[25] ZIGBEE ALLIANCE. **ZigBee specification**. 2006.

[26] HATLER, M. e CHI, C. **Wireless sensor networks for the oil & gas industry**. ON World Inc. 2005.

[27] RUIZ, L. B., CORREIA, L. H. A., VIEIRA, L. F. M., MACEDO, D. F., NAKAMURA, E. F., FIGUEIREDO, C. M. S., VIEIRA, M. A. M., MECHELANE, E. H., CAMARA, D., LOUREIRO, A. A. F., NOGUEIRA, J. M. S. e SILVA JR, D. C. **Arquiteturas para redes de sensores sem fio**. 200?

[28] AKYILDIZ, I. F., SU, W., SANKARASUBRAMANIAM, Y. e CAYIRCI, E. A survey on sensor networks. **IEEE Communication Magazine**. p. 102-114. Ago, 2002.

[29] DA SILVA, I. M. D. **Redes de sensores sem fio aplicadas em ambientes de petróleo e gás**. 2006. Monografia (Bacharelado em Engenharia da Computação). Universidade Federal do Rio Grande do Norte, Natal, 2006.

[30] PEREIRA, M. R., AMORIM, C. L. e CASTRO, M. C. S. **Tutorial sobre redes de sensores**. Rio de Janeiro: 200?

[31] SAKANE, S., ISHII, Y., TOBA, K. KAMADA, K. E OKABE, N. **A translation method between 802.15.4 and IPV6 nodes**. 2006.

[32] CIRRONET. Implementing ZigBee in existing industrial automation networks. **Sensors Expo 2005**. 2005.

[33] CULLER, D. **Secure, low-power, IP-based connectivity with IEEE 802.15.4 wireless networks**. Industrial Embedded Systems, 2007.

[34] ALVES, M. e TOVAR, E. **Real-time communications over wired/wireless PROFIBUS networks supporting inter-cell mobility**. Computer Networks 51, p. 2994-3012. Elsevier, 2007.

[35] KOUMPIS, K. HANNA, L., ANDERSSON, M. e JOHANSSON, M. **Wireless industrial control and monitoring beyond cable replacement**. PROFIBUS International Conference, 2005.

[36] WELANDER, P. **Topologies for wireless instrumentation**. Control Engineering. 2007. Disponível na Internet. Http://www. controleng.com. Acesso em: 15 de jan. 2008.

[37] KOUMPIS, K., HANNA, L. ANDERSSON, M. e JOHANSSON, M. **Technical article: a review and roadmap of wireless industrial control.** Disponível na Internet. Http://wireless.industrial-networking.com/articles. Acesso em: 16 de jan. 2008.

[38] WILLIG, A., MATHEUS, K. e WOLISZ, A. **Wireless technology in industrial networks**. Proceedings of the IEEE, v. 93, n. 6, p. 1130-1151. 2005.

[39] ARC ADVISORY GROUP. **Fieldbus solutions in the process industries to grow more than 22% annually**. Janeiro, 2007. Disponível na Internet. Http://www.arcweb.com. Acesso em: 19 de nov. 2007.

[40] HOSKE, M. T. Study: Fieldbus Foundation leads process industries. **Control Engineering Daily News Desk**. 2007. Disponível na Internet. Http://www.controleng.com. Acesso em: 02 de jan 2008.